ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

У. А. Төкеев, Б. Б. Ахметов

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ

Оқу құралы

Алматы
«Қазақ университеті»
2011

ББК 22.18 я73
Т50

Баспаға әл-Фараби атындағы Қазақ ұлттық университеті механика-математика факультетінің Ғылыми кеңесі және Редакциялық-баспа кеңесі шешімімен ұсынылған

П і к і р ж а з ғ а н д а р:

т.ғ.к., профессор ***А.З. Айтмағамбетов;***
т.ғ.д., профессор ***Д. Н. Шукаев;***
т.ғ.к., доцент ***Б. Бөрібаев;***
ф.м.ғ.к., доцент ***Д.Ж. Ахмед-заки***

Төкеев У. А., Ахметов Б. Б.

Т 50 Ақпараттық қауіпсіздікті басқару: Оқу құралы. – Алматы: Қазақ университеті, 2011. – 161 б.

ISBN 9965-29-757-6

Оқу құралы ақпараттар қауіпсіздігін басқару жағынан мемлекеттік тілде жазылған алғашқы әдістемелік құрал.

Оқу құралы 7 тараудан және бірнеше қосымшалардан тұрады. Әр тараудан соң шағын жаттығулар мен есептер берілген.

ББК 22.18 я73

ISBN 9965-29-757-6

КІРІСПЕ

Қазіргі таңда кез келген отандық компанияның дамуы оның ақпараттық қауіпсіздігін ұйымдастыруына байланысты. Отандық компаниялардың құпия ақпараттарды қорғау саласына ынталардың өсуі автоматтандыру қызметтерінің директорлары, қауіпсіздік қызметтерінің, отандық компаниялардың атқарушы директорларының келесі мәселелерді шешуге қызығушылығында:

– компанияның ақпараттық тәуекелдерін талдау және оны басқару;

– ұйым бизнесінің қарқындылығын бағалау;

– корпоративті жүйелерде ақпараттық қорғаудың экономикалық тиімділігін бағалау;

– ақпараттық қорғау жүйелерін бағалау;

– компанияның ақпараттық қауіпсіздік (АҚ) саласындағы инвестицияның қайтуын бағалау;

– ақпараттық қауіпсіздік қаржысын жоспарлау және басқару.

Аталған мәселелердің маңыздысы – ақпараттық тәуекелділіктерді талдау. Шынында, ақпараттық қауіпсіздік ұйымдастыруына жауапты адамдардың көбі өздеріне мынадай сұрақ қойған болар: «Ұйымның ақпараттық жүйе қауіпсіздігін басқаруын қалай бағалау және даму барысын қалай анықтау керек?». Қазіргі ақпараттық технологиялардың дамуы нормативті-құқықтық базалық құжаттардың пайда болуынан әлдеқайда алда. Сол себепті ұйымның ақпараттық жүйе қауіпсіздігін қамтамасыз етуі келесі сұрақтарға жауап талап етеді: қандай әдіс және көрсеткіштер бойынша біз жүйенің ақпараттық қауіпсіздік эффективтілігін бағалаймыз және соның ішінде ұйымның ақпараттық тәуекелділіктерін қалай бағалау немесе асыра бағалау? Сол себепті отандық компаниялар практикада халықаралық стандарттардың әдістерін қолданады (ISO 17799, ISO 9001, ISO 15408, BSI және т.б.), сондай-ақ ішкі ұйымаралық әдістерді қолдану, мысалы, иеліктің өзіндік құны (TCO), инвестицияның қайтуы (ROI).

Тәуекелді талдаудың қазіргі технологиялары отандық компаниялардың ақпараттық тәуекелдерінің деңгейін бағалау мүмкіншілігіне ие. Бұл ұйымның ақпараттық жүйесіне ақпараттық қауіпсіздік жағынан көп талаптар қойғанда керек. Бүгінгі таңда ақпараттық тәуекелділіктерді талдаудың бірнеше әдісі бар, соның ішінде отандық жағдайда қолдануға пайымдалған CASE қаражаттарын тарту. Ақпараттық тәуекелдерді талдау жақсы талдау әкеледі:

– ақпараттық қорғау бірнеше нұсқаларына қатысты «тиімділік-баға» жағынан салыстырмалы бағалау;

– ақпаратты қорғау үшін барабар қарсы әдіс таңдау;

– компанияның қалдық ақпараттық тәуекелдерін бағалау.

Ақпараттық қорғау облысындағы жаңа база негізінде құрылған тәуекелдерді талдау құрылғылары мүмкіндік береді:

– қазіргі корпоративті ақпараттық жүйелердің құрылымдық және объектілі-ориентілік модельдері;

– КАЖ элементтерінің жеке бөлігінің бөліктері ретінде қатер және тәуекелдер модельдері қарастырылады, осының арқасында ақпараттық жүйе қауіпсіздігіне қатерлі немесе тиімсіз тәуекелдерді болдыртпау;

– ақпараттық қауіпсіздік жүйелерінің неше түрлі моделін «тиімділік-баға» бойынша бір-бірімен салыстыру, ұйым алдындағы өз жұмысын толық атқару.

Оқу құралы жеті тараудан тұрады:

– Ақпараттық қорғау саласындағы тәуекелдерді талдау;

– Халықаралық стандарттар және тәуекелдерді басқару;

– Тәуекелдерді талдау технологиясы;

– Тәуекелдерді талдау құралдары;

– Қауіпсіздікті тексеру және тәуекелдерді талдау;

– Ақпараттық жүйелердің қорғалуын талдау;

– Шабуылдарды анықтау және тәуекелдерді басқару.

Бірінші тарауда отандық компаниялардағы ақпараттық қауіпсіздік ұйымдастыру барысындағы тәуекелдерді талдаудың рөлі және оны басқару жайлы айтылады. Компанияның ақпараттық қауіпсіздік жайлы халықаралық концепциялары қарастырылған.

Екінші тарауда тәуекелдерді басқару мен ақпаратты қорғау облысындағы стандарттарға шолу жүргізілген. Негізгі ақпараттық тәуекелдерді талдау және басқару бойынша артықшылықтар мен кемшіліктер көрсетілген.

Үшінші тарауда тәуекелді талдаудың негізгі технологиялар туралы, мүмкін болатын мәселелер және оның шешімі жайлы, сондай-ақ тәуекелдерді талдау әдістеріне мысалдар келтірілген. Бұл бөлімде осы салаға қатысты практикалық тәжірибе көрсетілген.

Төртінші тарауда тәуекелдерді талдау үшін қажетті инструменттік құрылғылар жайлы сөз болады.

Бесінші, алтыншы және жетінші тараулар шабуылдарды анықтау және қорғаныс міндеттерін талдау, тәуекелдерді талдау және оларды басқарудың бірегейлік қасиеттері көрсетілген.

Оқу құралының көп материалдары С.А. Петренко мен С.В. Симоновтың «Управление информационными рисками. Экономически оправданная безопасность» атты (М.: ДМК Пресс, 2005) кітабының материалдарына негізделген [1].

І ТАРАУ

АҚПАРАТТЫ ҚОРҒАУ САЛАСЫНДАҒЫ ТӘУЕКЕЛДЕРДІ ТАЛДАУ

1.1. Бизнестің ақпараттық қауіпсіздігі

Қазіргі таңда корпоративтік ақпараттық жүйелердегі (КАЖ) ақпараттық қауіпсіздікті қамтамасыз ету жайлы күннен-күнге көптеген компьютерлік басылымдардың бетінде жариялануда. Бірақ әлі де техникалық шешімдерді шешуге, соның ішінде ақпаратты қорғаудың белгілі аппараттық және программалық құралдардың ақауларын талдауға маңызды көңіл бөлінеді. Компанияның АҚ қамтамасыз ету барысында ақпаратты қорғау тактикасы мен стратегиясы, тұжырымдамасы мен саясаты аз мөлшерде қозғалады, сондай-ақ компанияның штаттық және штаттық емес КАЖ қызмет жағдайларының ақпараттық ресурстарын қорғау жоспарлары да аз қарастырылмайды. Сонда да отандық бизнес өкілдері үшін бұл мәселе өзекті болып табылады.

Бұл мәселе, көбінесе, техникалық мамандардың немесе техникалық тамыры бар мамандардың ортасында талқыланады. Компанияның бизнес-басқармасының пайымдауынша, компанияның ақпараттық ресурстарына төнетін қауіп және КАЖ техникалық ақаулықтары байқалмайды, сол себепті КАЖ ақпараттық қауіпсіздікпен қамтамасыз ету бұлыңғыр болып көрінеді. Бірақ мына мәселенің қойылуы анық: корпоративтік жүйенің ақпараттық қорғауына ақша жұмсау тиімді ме? Отандық автоматтандыру қызметтерінің директорлары мен басшылары (*CIO,* Chief Information Officer), атқарушы директорлар (CEO, Chief Executive Officer), ақпараттық қауіпсіздік қызметтерінің басшылары (CISO, Chief Information Security Officer) бұл мәселе шешілуін қалайды. Сонымен, ақпараттық қауіпсіздік корпоративтік бизнес процестерінің бір бөлігі болу үшін не істеу керек? Басқа сөзбен айтқанда, АҚ бизнес тұрғысынан қалай елестетуге болады?

Ол үшін алдымен АҚ бизнес мақсаттарын анықтап алу қажет. Бизнесті автоматтандырудың негізгі двигателі – жаңа ақпараттық технологияларды қолдану арқылы нәтижелі және бәсекеге қабілетті болуына ұмтылу және өз моделін жетілдіру. Мұндай ұмтылыс толығымен түсінікті: бәсекеге қабілетті шынайы механизмдер көп қалмады, көбі әлдеқашан таусылған, ал ақпараттық технологиялар, шындығында, таусылмас мүмкіндіктер ұсынып отыр. Бүгінгі таңда бизнестің автоматтандыруына, динамикалық

түрде дамуына үлкен әлеует салынғанына ешкім күмән келтірмейді. Жұмыстың нәтижелілік және шапшаңдығын салыстыру жеткілікті, мысалы корпоративтік электрондық поштаны мыңдаған хатшылар мен машинисткалар ретінде салыстыруға болады, CAD/CAM/CAE-жүйелерінің көмегімен қиын техникалық әзірлеулердің сапасы мен мерзімін және дәстүрлі кульмандардың көмегімен және т.б. КАЖ бизнестегі мақсаты үлкен, жай, қатесі көп бизнес процестерді жеңілдету, тездету немесе ыңғайлы қылу. Кез келген бизнес қарамағындағы техникалық жүйе бизнеске бір қызмет жасауы қажет. Қызметтің түрі көп: домендік пеш «қызмет көрсетеді», темірді балқытады, транспорттық цех жүктерді тасымалдайды, завод асханасы жұмысшыларды тағаммен қамтамасыз етеді және т.б. КАЖда осындай техникалық жүйе болғандықтан, бизнеске өз қызметін көрсетеді, дәл мұндай жағдайда ол ақпараттық. Бұл қызмет бизнеске қажетті ақпаратты қабылдауға, керек уақытта, керек жерде, яғни бизнесті басқаруға арналған ақпаратпен қамтамасыз ету болып табылады.

Ақпарат бизнестің бір маңызды элементі болып келе жатыр. Бизнес тұрғысынан қарағанда ақпарат деген не? Былай қарағанда, бұл формальдылардың жиынтығы сияқты (құрылымдық, сөрелерге рет-ретімен қойылған, іздеуге және елестетуге арналған құрылымы бар) бизнестің өзін-өзі тануы. Соның өзінде ақпарат мағынасының төңірегінде тек статикалық ақпарат қорын елестетіп қоюға болмайды, мысалы былтырғы жылғы бухгалтер баланс немесе кейбір құрылғылардың ағымдағы баптауы, немесе компанияның динамикалық ақпараттық процестерінің программаланған бизнес-логика жұмыстарының атақты қосымшалар ішінде ERP, CRM, каталогты қызмет және т.б. электрондық құжат аралық өңделуі.

Қазіргі таңда кез келген үлкен компанияның басшысы ақпаратпен ғана жұмыс жасайды, соның негізінде шешім қабылдайды. Осы ақпаратты күрделі жүйелік ұйымның төменгі сатылы қызметкерлері дайындайды. Төменгі сатылы қызметкерлердің өнім өңдеу немесе қызмет көрсетуден басқа басшылыққа ақпарат беретіні жайлы беймәлім болуы мүмкін. Біздің ойымызша, бизнесті автоматтандырудың маңызы да осында, компанияның қызмет көрсету деңгейі мен қабаттарындағы ақпараттық ағындарды басшылық назарына тездетіп компанияның басшылығына тек қажетті, анықталған, сенімді ақпарат жету үшін. Корпоративтік АҚ жүйесінің негізгі мақсаты – ақпараттың шынайылығына кепілдік беруінде, басқа сөзбен айтқанда, КАЖ ақпараттық жүйесінің сенімділігіне кепілдік беру.

Отандық бизнестің кез келген өкілінен, сіз жүз мың долларыңызды бес желі аралық экран және жүз антивирустық лицензия сатып алатын ба едіңіз деп сұрайық. Содан соң, сіз жүз мың долларыңызды өзіңіз жайлы ақпараттың қорғалуына және компанияңыздың қызметінің қорғалуына жұмсар ма едіңіз деп сұрасақ. Бірінші сұраққа көбіне тән «Ақшам жоқ» деген жауапқа немесе қарама-қарсы «Не үшін?» деген сұраққа кенелесіз.

Ал екінші сұрақтың жауабына «Қанша мерзімде үлгереміз? Сіз баяғыдан қайда болғансыз?», «Не үшін аз ақша? Менің бизнесім осыншама аз тұрады ма?» деген сұрақтарға кенелесіз.

Одан басқа бұл жерде тағы бір қызық сұрақ туады: «Не үшін жүз мың, неге елу емес немесе айтарлық төрт жүз жетпіс бес емес?». Осы жағдайда CIO, CEO, CISO бизнеске түсінікті, экономикалық тұрғыдан дәйектелген жауап бергені дұрыс. Бизнестегі АҚ жүйесінің құнын түсіндіріп, анықтау.

Корпоративтік жүйенің ақпараттық қорғауын талдау арқылы құнын анықтауға болады ма? Соңғы кезде АҚ байланысты баспада жаңа тақырыптар пайда болғаны мәжбүр: АҚ қауіптерін талдау, ақпараттық тәуекелдерді талдау, қауіпсіздік жүйесінің құнын бағалау, инвестицияның қайту бағасын анықтау және т.б. Мұның барлығы ақпараттық қауіпсіздіктің бір экономикалық құрылғысы ретінде сұрақтарға жауап береді: «Неге жүз мың?». Корпоративтік ақпараттық қауіпсіздік жүйесінің құнын анықтауды қарастырайық. Біздің ойымызша, мұны анықтаудың екі тәсілі бар.

Бірінші тәсілді ғылыми деп атайық, бірінші осы саланы тану, практикада қауіпсіздік әдістері мен қажетті құрылғыларын пайдалану арқылы метрикаларын анықтау, ол үшін компания басшысын қорғалған ақпаратының құнын анықтауға келістіру, содан соң оған төнген қауіптер мен ақау жерлерін анықтау. Мұндай бағалаудың нәтижесіне АҚ облысындағы *CIO* және *CISO* болашақтағы қызметі бағынышты. Егер ақпарат ештеңе тұрмаса, компанияның ақпараттық активтеріне ешқандай қауіп төнбесе, потенциалдық зиян минималды болса және ұйым осыны қолдаса, АҚ мәселесімен айналыспай-ақ қойған дұрыс. Егер ақпарат белгілі бір ақша тұрса, қауіптер мен потенциалдық зиян белгілі болса, онда корпоративтік АҚ жүйесінің бағасы да белгілі болады. Сонда компания басшылығына АҚ мәселелерін түсіндіруге және корпоративтік ақпараттық қорғау жүйесін құруға әрі соның көмегіне сенуге болады.

Екінші тәсіл (практикалық деп атайық) келесіден тұрады: корпоративтік ақпараттық қорғау жүйесінің құнын табудың басқа жолын табу. Басқа ұқсас салаларда да басқа жолдары бар. Мысалы, авто сақтандыру саласында жалпы бағалау қызмет құны өз бағасының 5-15%-ға дейінгі құнын құрайды, оның жүрілгеніне, жүргізушінің жүргізу тәжірибесіне, жүру интенсивтілігіне, жолдың жағдайына қарай және т.б. жолдармен анықтайды.

Компания АҚ сақтандырумен айналыспай-ақ қойса болады, бұл қауіптің өзін ақтау мүмкін емес екені белгілі. Корпоративтік ақпараттық қауіпсіздік жүйе саласына біраз ақша жұмсауға болады, бірақ бір күні компанияның құпия ақпаратын ұрлап кететіндей бір ақау болуы мүмкін. Сондықтан ақпараттық қорғау облысындағы эксперт-практиктер жақсы жағдай тапты, АҚ жүйесі КАЖ бағасының ақпараттық құпиялығына байланысты 10-20%-ды құру қажет. Осы сенуге болатын практика негізін-

дегі бағалау болып табылады (best practice). Ал «Корпоративтік ақпараттық қауіпсіздік жүйесін құруға неге жүз мың доллар керек?» деген сұраққа «Бүгінгі таңда КАЖ құны бір миллион доллар болды» деп жауап береміз.

Екнші тәсіл қатесіз деп айту қате болар. Мұнда басшылыққа АҚ мәселелері жайлы түсіндіру қиын болар, бірақ АҚ құнын ойланбастан бағалауға болады.

1.2 Ақпараттық қауіпсіздік жүйесінің дамуы

Кез келген отандық компанияның дамуымен (оның ақпараттық активтерінің өсуімен) қоса оның ақпараттық қауіпсіздік қызметі де дамиды. Компанияның жоғарғы менеджментінің маңызды атқаратын қызметі – ақпараттық қауіпсіздік қызметінің стратегиясы мен тактикасын анықтау. Шынында, қазір компанияның ақпараттық қауіпсіздік саясатын ұйымдастыру ақпараттық қауіпсіздік саласындағы техникалық немесе ұйымдастырушылық облысына ғана қатысты емес, сонымен қатар жақсы кадрға да байланысты. Белгілі тезисті еске алайық: «Кадр бәрін шешеді!». Компания қызмет барысындағы ақпараттық қауіпсіздік рөлін және орнын көрсетейік, сондай-ақ осы қызметтің қызметкерлеріне білікті талаптар құрайық.

Компанияның TOP-менеджментінің ақпараттық қауіпсіздік режимін ұйымдастыру барысындағы құрылымы 1.1 суретіте көрсетілген.

KPMG 2002 жылғы зерттеуіне қарағанда компанияның жоғарғы басшылығының қолдауына ие болып, батыс компанияларының көбінде АҚ бөлек бөлім айналысады. Сондай-ақ табысты компаниялардың тең жартысында АҚ директорлар кеңесіне қарайды, бұл қаржылық тұрғыдан дұрыс. Шынында, TOP-менеджменттің тікелей қатысуымен компанияның АҚ облысындағы мақсаттары мен шешу жолдары компания бизнесіне қатерсіз болуы маңызды. Сондай-ақ тек компания басшылығы ғана қауіпсіздік саласын инвестициялай және қажетті ресурстармен жабдықтай алады.

CISO-ның негізгі жұмысы - компанияның технологиялық, өндірістік және ақпараттық тәуекелдерін бағалау және оны басқару. Бұл маманның компания тәуекелдерін анықтап, оларды компания даму жолына сай басқару қажет. Компанияның жұмыс істеу саласы, сонымен қатар компанияның көлемі және ақпараттық активтерінің құны қосымша ерекшеліктер енгізеді.

CISO негізгі қызметтері келесілер болуы мүмкін:

– компанияның ақпараттық қауіпсіздік тұжырымдамасын және саясатын, регламентін, корпоративтік стандартын, басқару нұсқауларын құру;

– компанияның ақпараттық активтерінің біліктілік принциптерін өңдеу және олардың қауіпсіздігін бағалау;

– ақпараттық тәуекелдерді бағалау және оларды басқару;

– компания қызметкерлерінің АҚ қамтамасыз ету жолдарын оқыту, компания қызметкерлерінің АҚ жайлы білімдерін дамыту;

– компания менеджерлеріне ақпараттық тәуекелдерді басқару жайлы кеңес беру;

– компания бөлімдерінің жеке қауіпсіздік саясаты және регламенттерін ұйғару;

– компания бизнесінің дамуы және тәуекелдерді бағалау үшін жұмыс тобы немесе эксперт кеңесінің ішінде жұмыс істеу;

– компанияның автоматтандыру және сапа қызметтерінің жұмысын қадағалау, олардың құжаттарын тексеру құқығына ие болу арқылы;

– физикалық қауіпсіздік қызметімен екеуіне де қатысты салада бірге жұмыс істеу, мысалы ғылыми зерттеу жұмысының құпиялығын қамтамасыз ету және қызметкерлердің кіріп-шығуын қадағалау;

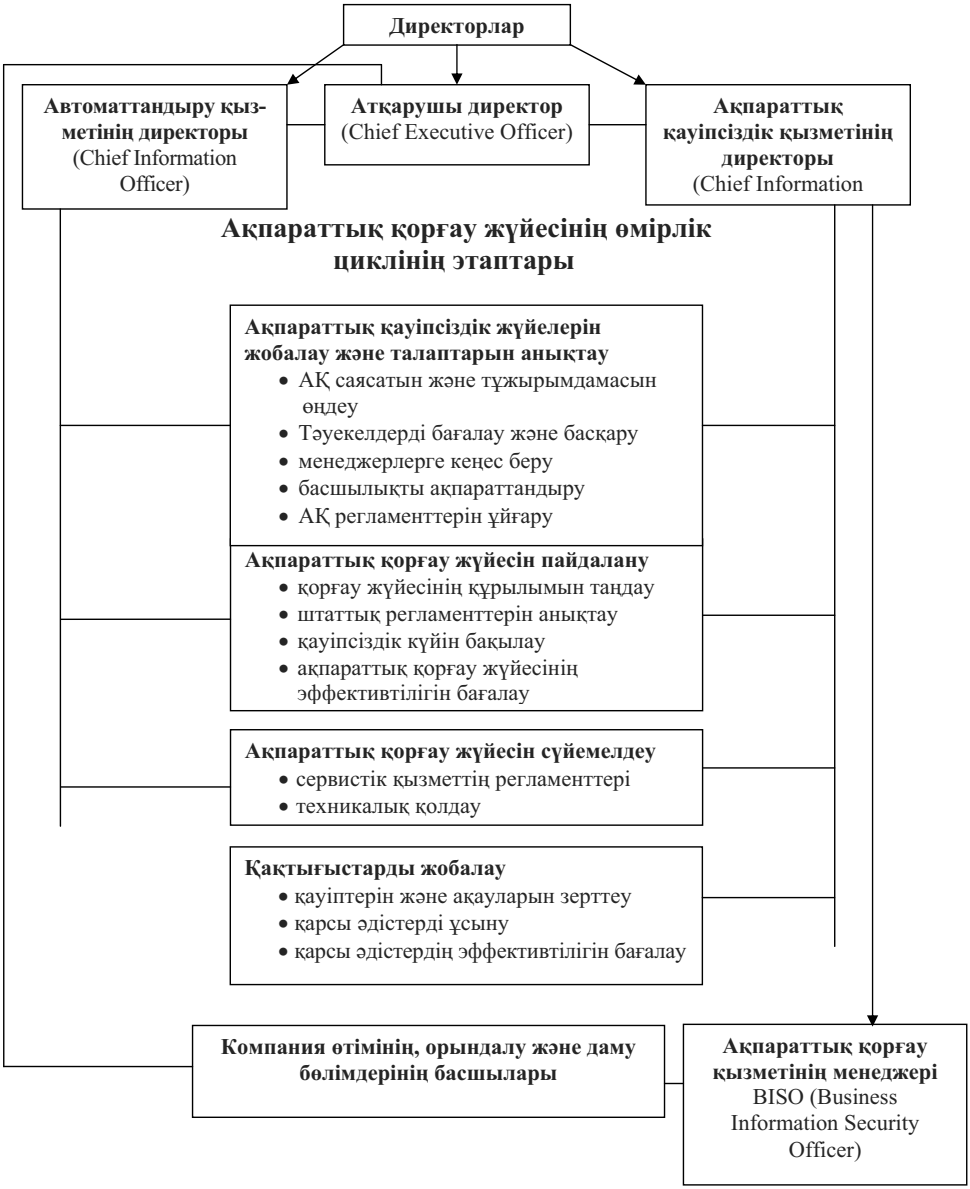
– қызметкерлерді жұмысқа алу барысында кадрды таңдау қызметімен бірге жұмыс істеу;

– ақпараттық қауіпсіздік саласына қатысты төтенше жағдайлар болғанда оларды жою іс-шараларын ұйымдастыру;

–компания басшылығын тұрақты шолулар мен компанияның ағымдағы ақпараттық қауіпсіздігі жайлы ақпараттандыру, қауіпсіздік саясаты нәтижелерін баяндау;

– компания менеджерлеріне АҚ жайлы ақпараттық қолдау көрсету, көбіне ақпараттық қорғау сферасындағы нормативтік заңдардың өзгеруі, техникалық жаңалықтар және т.б. жайлы.

Ақпараттық қауіпсіздік қызметінің жетекшісі (CISO) компания басқарудың жоғарғы эшелонында қызмет еткені дұрыс деп қарастырылады, себебі ақпараттық технологиялардың дамуына байланысты, қаскүнемдердің әртүрлі қастық белсенділіктеріне, заң ережелерінің өзгеруіне, сондай-ақ бизнес серіктестерінің күтуіне байланысты. Бұл кездің өзінде бизнестің көзқарасы ақпараттық қауіпсіздікті қамтамасыз етуге қарама-қайшы келуі мүмкін. Осы жағдайда CISO отандық бизнес өкілдеріне техникалық ақауларды түсінікті тілде жеткізе алуы керек. Сол үшін CISO негізгі және қосымша (MCSE, CISA, ABCP сертификациясы және т.б.) білімдерге, сондай-ақ ақпараттық қорғау саласында (кемінде 3-5 жыл) тәжірибесіне қоса тұлғалық қасиеттерге ие болуы қажет. Мысалы, еңселі ойлау қабілетіне, стратегиялық және операциялық менеджмент облысында қабілеттіліктерге, ұйымға шынайылықпен қарау және т.б. қасиеттерге ие болу керек. Бұл үшін тек техникалық, экономикалық немесе басқару мамандықтары жеткіліксіз. Сол үшін CISO бағытын ақпараттық қорғау саласында біраз тәжірибесі бар талдаушылар немесе аудиториялар тыңдауы мүмкін.



1.1-сурет. Компанияның ақпараттық қауіпсіздігіне жауапты TOP-менеджментінің ұжымдық құрылымы

1.3 Ақпаратты қорғаудың халықаралық практикасы

Ақпараттық қауіпсіздігін қамтамасыз етуде мекеменің ақпараттық тәуекелін талдау және оларды басқару есептеріне көп көңіл бөлінеді. Ақпараттық қауіпсіздігін қамтамасыз ету режимі жұмыстарын және тәуекелдерді басқару және талдау есептерінің орны мен рөлін қарастырайық.

Мекеме өлшемі мен оның ақпараттық жүйесінің сипатына қарамастан ақпараттық қауіпсіздік режимін қамтамасыз ету жұмыстары, әдетте келесі кезеңдерден тұрады (1.2-сурет):

- қауіпсіздік саясатын қалыптастыру;
- ақпарат қауіпсіздігі жүйесінің саласын анықтау және оның құрылу мақсаттарын нақтылау;
- тәуекелдерді бағалау;
- ақпарттық қауіпсіздік режимін қамтамасыз ететін контршараларды таңдау;
- тәуекелдерді басқару;
- ақпарат қауіпсіздігін басқару жүйесінің аудиті.

Аталған кезеңдердің әрқайсысына толық ашылған сипаттама төменде берілген.

Ереже бойынша қауіпсіздік саясатын анықтауда бірқатар тәжірибелік қадамдар келтіріледі:

1-қадам. Ақпараттық қауіпсіздік саласында ұлттық, халықаралық жетекші құжаттар мен стандарттарды таңдау. Олардың негізінде мекеменің ақпараттық қауіпсіздік саясатының қосымшалары мен негізгі талаптарын қалыптастыру:

- есептеу техникасы құралдарына, программалар мен мәліметтерге қатынасты және антивирустік қорғауды басқару;
- қосымша көшіру сұрақтары;
- жөндеу және қалпына келтіру жұмыстарын жүргізу;
- ақпараттық қауіпсіздік саласындағы келеңсіз оқиғалар жөнінде ақпарат беру.

2-қадам. Ақпараттық тәуекелдерді басқаруды қалыптастыру және компьютерлік ақпараттық жүйелердің (КАЖ) қорғалу деңгейін таңдау жөнінде шешім қабылдау. Шетел стандарттарына сай қауіпсіздік деңгейі минималды (базалық) немесе жоғары болуы мүмкін. Осы қауіпсіздік деңгейлеріне ақпараттық тәуекелдерді талдаудың минималды (базалық) және толық нұсқасы сай келеді.

3-қадам. Келесі негізгі деңгейлер бойынша ақпаратты қорғау жөнінде контршараларды реттеу: администрациялық, процедуралық және бағдарлама-техникалық.

4-қадам. Ақпараттық қауіпсіздік саласындағы стандарттарға сәйкес КАЖ сертификация мен аккредитация қатарын орнату. Жетекшілік деңгейде ақпарат қауіпсіздігі тақырыбында отырыстар кезеңділігін та-

ғайындау, соның ішінде ақпараттық қауіпсіздік саясатының қойылымдарын, ақпараттық қауіпсіздік саласында ақпараттық жүйе тұтынушылар категориясын оқыту қатарын кезеңді түрде қарап отыру.

1.2-сурет. Ақпараттық қауіпсіздік режимін қамтамасыз ету. Негізгі кезеңдер

Мекеме қауіпсіздік саясатын қалыптастыруда ең аз реттелген кезең екені белгілі. Алайда соңғы кездері бұл жерде ақпаратты қорғау мамандарының күштері осыған бағытталған. Нәтижесінде осы кезеңді жоғары деңгейде қалыптастыру мүмкін. Бұған мысал: «Автоматтандырылған ақпараттық жүйелерді қауіпсіздік саясатын басқару». Онда келесілер қарастырылады:

- қауіпсіздік саясатының жалпы қойылымдары;
- КАЖ қауіпсіздігінің өмірлік айналымы;
- ақпараттық қауіпсіздік саласында минималды (базалық) талаптар.

Келесі кезең – ақпарат қауіпсіздігін басқару жүйесінің аймағын (шекара) анықтау және оның құрылу мақсаттарын нақтылау.

Бұл кезеңде ақпараттық қауіпсіздік режимін қамтамасыз ету керек жүйенің шекарасы анықталады. Сәйкесінше ақпараттық қауіпсіздікті басқару жүйесі осы шекарада құрылады. Жүйе шекарасын сипаттауды келесі жоспар бойынша орындау ұсынылады:

- Ұйымның құрылымы. Бар құрылымдар мен өлшемдерді көрсету. Оны автоматтандырылған жүйе құруға орай енгізу болжанады.

- Қорғауға келетін ақпараттық жүйе ресурстары. Келесі класты автоматтандырылған жүйе ресурстарын қарастыру керек: есептеу техника құралдары, мәліметтер, жүйелік және қолданбалы ПҚ. Мекеме тұрғысынан барлық ресурстар бағалы болып табылады. Оларды бағалау үшін критерийлер жүйесі таңдалып, осы критерийлер бойынша нәтиже алу әдістемесі болу керек.

- Шешілетін есептер мен ақпаратты өңдеу технологиясы. Шешілетін есептер үшін ақпаратты өңдеу модельдері құрылуы тиіс.

- Қолданатын инфрақұрылым мен есептеу техника құралдарын орналастыру.

Ереже бойынша бұл кезеңде ақпараттық жүйе шекарасы көрсетілетін құжат құрылып, мекеменің қорғалатын ақпараттық ресурстары санамаланады, мекеменің ақпараттық активтерінің құндылығын бағалау әдістемесі және критерийлер жүйесі келтіріледі.

Тәуекелді бағалау есебін қою кезеңіне мекеменің ақпараттық тәуекелдерін бағалау әдістемесіне талаптар негізделеді.

Қазіргі кезде тәуекелдерді бағалауға әртүрлі көзқарастар бар. Көзқарасты таңдау мекемеде ұсынылатын ақпараттық қауіпсіздік режим талаптарына, есепке алынатын қауіп сипатына, ақпаратты қорғау жөнінде потенциалды контршаралардың тиімділігіне байланысты. Жеке жағдайда ақпараттық қауіпсіздік режиміне минималды немесе базалық және жоғары немесе толық талаптарды бөліп көрсетеді.

Ақпараттық қауіпсіздік режимінің минималды талаптарына ақпараттық қауіпсіздіктің базалық деңгейі сәйкес келеді. Мұндай талаптар типтік жобалық шешімдерде қолданылады. Вирустар, құрылғының істен шығуы, заңсыз қатынас сияқты ықтимал қауіптің минималды жиыны көрсетілетін стандарттар мен сипаттар бар. Осы қауіптерді бейтараптау үшін ресурстың осалдығы мен жүзеге асу ықтималдығына қарамастан контршаралар

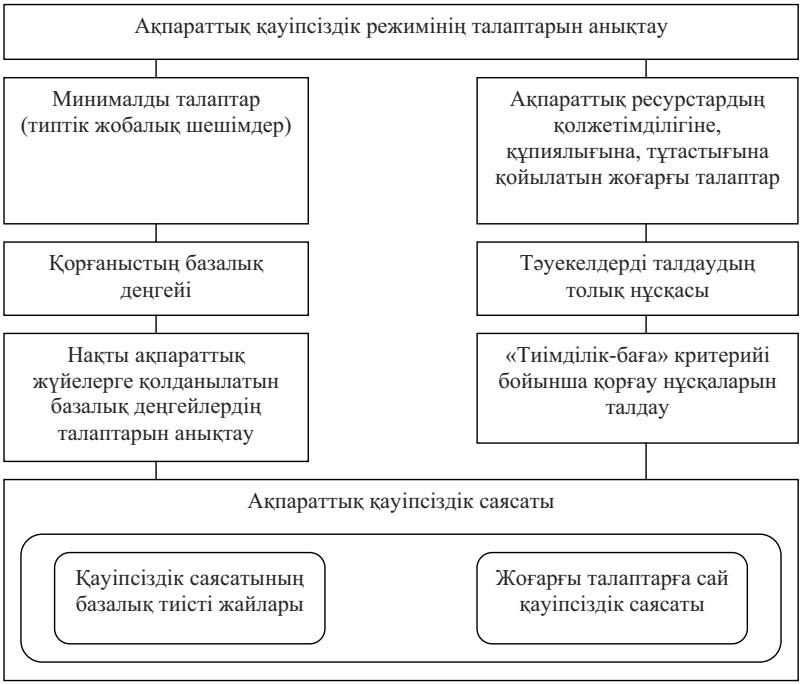
қолданылуы керек. Осылайша, базалық деңгейде қауіп сипаттамаларын қарастыру міндетті емес. Осы саладағы шетелдік стандарттар 2-тарауда қарастырылады.

Ақпараттық қауіпсіздік режимінің бұзылуы ауыр зардаптарға әкелетін жағдайда ақпараттық қауіпсіздік режиміне талаптардың базалық деңгейі жеткіліксіз және қосымша ауырлатылған талаптар ұсынылады. Қосымша ауырлатылған талаптарды қалыптастыру үшін:

- ресурстардың құндылығын анықтау;
- зерттелетін ақпараттық жүйелерде маңызды болатын қауіп тізімін стандартты жиындарға қосу;
- қауіптер ықтималдықтарын есептеу;
- ресурстардың осалдылығын анықтау;
- зұлымдардың әрекетінен болатын потенциалды шығынды бағалау.

Қосымша талаптарды таңдаудың басқа жолдары 3-тарауда көрсетілген.

Қауіпсіздіктің базалық және жоғары деңгейлерін қамтамасыз ету әдіс-темелеріндегі айырмашылыққа қарамастан ақпарат қауіпсіздігін ұйымдастырудың бірыңғайлылығы жөнінде сөз қозғаған жөн (1.3-сурет).



1.3-сурет. Ақпараттық қауіпсіздік режимін ұйымдастыру

Тәуекелдерді басқару кезеңінде тәуекелдерді басқарудың бірқатар стратегиясы қалыптасады. Мысалы, мұнда мекеменің ақпараттық тәуекелдерін басқаруға келесі көзқарастар мүмкін болады:

- тәуекелді азайту;
- тәуекелден ауытқу;
- тәуекел сипатының өзгерісі;
- тәуекелді қабылдау.

Аталған көзқарастарды толығырақ қарастырайық.

Тәуекелді азайту. Көптеген тәуекелдерді аса қарапайым және арзан контршаралардың есебінде төмендетуге болады. Мысалы, парольдерді дұрыс басқару заңсыз қатынас тәуекелін төмендетеді.

Тәуекелден ауытқу. Тәуекелдің көптеген түрлерінен ауытқуға балады. Осылайша, мекеменің Web-серверін жергілікті желі шегінен шығару Web-клиент тұрғысынан жергілікті желіге заңсыз қатынас тәуекелін болдырмауы мүмкін.

Тәуекел сипатының өзгерісі. Егер тәуекелден ауытқу немесе оны тиімді төмендету болмаған жағдайда бірқатар сақтандыру шараларын жүргізуге болады:

- құрылғыны өрттен сақтандыру;
- ЕТҚ жеткізушілермен ойда жоқ оқиғалардан болатын шығындарды өтеуі жөнінде шарт жасасу.

Тәуекелді қабылдау. Көптеген тәуекелдерді ескерілмейтіндей аз өлшемге жеткізуге болмайды. Тәжірибеде контршаралардың стандартты жиынын қабылдаудан кейін тәуекелдер азаяды, бірақ әлі де маңызы болады. Тәуекелдің қалдықты өлшемін білген жөн.

Мекеменің есепке алынатын ақпараттық тәуекелдеріне қолданылатын осы кезеңді орындау нәтижесінде тәуекелдерді басқару стратегиясы ұсынылуы тиіс.

Келесі кезең АҚ режимін қамтамасыз ететін контршараларды таңдау болып табылады. Бұл қадамда ақпараттық қауіпсіздікті қамтамасыз етудің нормативті-құқықтық, ұйымдастырушылық-басқарушылық, технологиялық және аппаратты-бағдарламалық деңгейлерінде құрылған ақпаратты қорғау үшін әртүрлі контршаралар кешені таңдалады. Одан әрі ұсынылған контршаралар кешені ақпараттық тәуекелдерді басқару стратегиясына сәйкес жүзеге асады. Егер тәуекелдерді талдаудың толық нұсқасы келтірілсе, онда әрбір тәуекел үшін қосымша ақпаратты қорғау контршаралар кешенінің тиімділігі бағаланады.

Ең соңында АҚ басқару жүйесінің аудиті кезеңінде ақпаратты қорғау жөнінде таңдалған контршаралардың мекеме қауіпсіздігінің саясатында жарияланған бизнес есептері мен мақсаттарына сәйкестігін тексереді, қалдықты тәуекелдерді бағалау, қажет болса, тәуекелді тиімділеу орындалады. 5-тарауда ақпараттық қауіпсіздік талаптарына сәйкес ақ-

параттық технологиялар сертификациясы мен аудит сұрақтары қарастырылған.

1.3.1 Symantec LifeCycle Security моделі

Ақпараттық қауіпсіздік режимінің мүмкін болатын мысалы ретінде Axent компаниясы ұйымдастырған Lifecycle Security (Axent пен Symantec бірігуі нәтижесінде модель Symantec Lifecycle Security атауын алды) моделін қарастырайық. LifeCycle Security моделі ақпаратты қорғаудың корпоративті жүйесін құру және жалпы ақпараттық қауіпсіздікті ұйымдастыру кезеңдерін сипаттап, реттейді. Онда көрсетілген процедуралар жиынын орындау ақпаратты қорғаумен бйланысты есептерді жүйелі шешуге және ақпаратты қорғау шаралары мен техникалық және ұйымдық құралдарға кеткен шығындарды бағалауға мүмкіндік береді. Бұл тұрғыда Lifecycle Security идеологиясы шешімдердің арнайы бөліктерін енгізуге негізделген «нүктелік шешім» тактикасына қарсы қойылған. Алдын ала талдаусыз және жоспарсыз мұндай тактика корпоративті ақпараттық жүйеде ақпаратты қорғаудың әртүрлі мәнді құралдар жиынының пайда болуына әкеледі. Олар өзара сәйкес келмейді, бұл мекеменің ақпараттық қауіпсіздігін қамтамасыз ету мәселесін тиімді шешуге мүмкіндік береді.

Lifecycle Security моделі негізгі жеті кезеңнен тұрады (1.4-сурет).

1.4-сурет. LifeCyde Security моделінің кезеңдері

Ақпарат саясаттары, стандарттар, процедуралар мен өлшемдер. Бұл кезеңде ақпараттық қауіпсіздікті қамтамасыз ету жөнінде шаралар негізінде жүзеге асатын шектері мен өлшемдері анықталады және алынған нәтижені бағалау үшін критерийлер беріледі. Бұл жерде стандарт дегеніміз тек қана ақпараттық қауіпсіздік саласындағы мемлекеттік және халықаралық стандарттар емес, сонымен қатар бірқатар жағдайларда құрылушы

корпоративті ақпаратты қорғау жүйесінің жобасына жеткілікті мөлшерде әсер ететін корпоративті стандарттар да жатады. Ұсынылған өлшемді енгізу ақапаратты қорғау жөнінде жұмыстарды өткізгенге дейінгі және кейінгі жағдайын бағалауға мүмкіндік береді. Сонымен қатар өлшем жүргізу КАЖ қорғанысын өлшеу ретін және өлшеу бірліктерін орнатады, бұл мекеменің АҚ-ға кеткен шығын мен енгізілген ақпаратты қорғаудың корпоративті жүйесінен түскен әсерді сәйкестендіруге мүмкіндік береді.

Тәуекелді талдау. Бұл кезең өз кезегінде қорғау жүйесін тиімді басқаруды орнату мен қолдаудағы түйінді нүкте болып табылады. Тәуекелді талдаудың мәліметтері бойынша ақпараттық жүйе құрамы мен құрылымын толығырақ сипаттауға, мекеменің дұрыс жұмысына маңыздылығы бойынша қолда бар ресурстарды реттеуге, жүйе осалдығын теңестіріп, ондағы қауіптерді анықтауға мүмкіндік береді.

Қорғау жүйесін қорғаудың стратегиялық жоспары. Тәуекелді талдау нәтижелері қорғау жүйесін қорғаудың стратегиялық жоспарын құрудың негізі болып табылады. Мұндай жоспардың болуы бюджет пен ресурстарды маңыздылық бойынша реттеуге, ақпаратты қорғау құралдарын таңдап, оларды енгізу тактикасы мен стратегиясын ұйымдастыру.

Шешімдерді таңдау және енгізу. Ақпаратты қорғау саласында шешімдерді қабылдаудың нақты критерийлері мен енгізу бағдарламасының болуы мекеменің ақпараттық жүйесінің дамуына кедергі келтіріп, «ауыр жүк» болатын ақпаратты қорғау құралдарына қол жеткізу мүмкіндігі азаяды. Бұл кезеңде жеткізушілермен келген сервистік қызмет көрсетуін ескерген жөн. Сонымен қатар құрылған жоспарларды орындаудағы және ақпаратты қорғау саласындағы қойылған мақсатқа жетудегі шешімді енгізудің рөлін анықтау керек.

Персоналды оқыту. АҚ саласындағы білім мен техникалық тренингтер мекеменің қауіпсіз есептеу ортасына қызмет көрсетуді құру үшін керек. Персоналды оқытуға кеткен шығындар КАЖ қорғау шараларындағы сәттілігімен ақталады.

Қорғау мониторингі. Аталған кезең корпоративті ақпараттық жүйеге басып кірулерді анықтап, ақпаратты қорғау жүйесінің тиімділігін оперативті түрде бақылап отыруға мүмкіндік береді.

Келеңсіз оқиғаларды сезу әдістерін құру және қалпына келтіру. Алдын ала құрылмаған және дайындалмаған қауіпсіздік саласындағы келеңсіз оқиғаларды сезіну процедуралары болмайынша зұлымның әрекеттеріне қарсы шабуылдарды табу жағдайында оларға қорғанудың тиімді шаралары қарсы қойылатынына және жүйенің жұмыс қабілеті тез қалпына келтірілетініне кепілдік беру мүмкін емес.

Lifecycle Security моделінде жоғарыда аталған кезеңдер өзара байланысты және ақпаратты қорғаудың корпоративті жүйесін жаңғырту процесінің үздіксіздігі болжанады. Осы модельдегі ақпараттық тәуекелдерді

талдау кезеңіне маңызды рөл бөлінген. Тәуекелдерді келесі жағдайларда жүргізу ұсынылады:

- ақпараттық жүйені және оның құрылымындағы өзгерістерді жаңарту;
- КАЖ құрудың жаңа ақпараттық технологиясына көшу;
- компанияда жаңа қосылуларды ұйымдастыру (мысалы, филиалдың жергілікті желісін орталық кеңсенің желісіне қосу);
- ғаламдық желіге қосылу (ең алдымен Интернетке қосылу);
- бизнесті енгізу тактикасы мен стратегиясын өзгерту (электронды дүкендерді ашу);
- ақпараттық қорғаудың корпоративті жүйесінің тиімділігін тексеру.

КАЖ ақпараттық тәуекелдерін талдаудың негізгі бөліктері:

- жүйені толық құжаттандыру, соның ішінде бизнес үшін маңызды қосымшаларға көңіл бөлу;
- ұйымның аймақтық жұмыстан және жүйенің құрылымдық элементтерден, сақталатын және өңделетін мәліметтер қауіпсіздігінен тәуелділік дәрежесін анықтау;
- осал тұстарын анықтау және ескеру;
- потенциалды қауіптерді анықтау және ескеру;
- ақпараттық тәуекелдерді ескеру және бағалау;
- жалпы КАЖ және ақпарат иелеріне потенциалды шығындарды бағалау.

КАЖ-дың қорғаныс шаралары мен өлшеу жүргізу тәуекелдерді талдау процедурасын анықтайды. Екінші жағынан, ақпараттық тәуекелдерді талдау нәтижелері ақпаратты қорғаудың корпоративті жүйесінің қайта құрылуына бастапқы шарттарды қалыптастырады.

1.4 Тәуекелдерді талдау есептерінің қойылымы

АҚ қамтамасыз ету есебінің қойылымы үлкен шектерде орын алуы мүмкін. Сәйкесінше, тәуекелді талдау есебі де орын алуы мүмкін.

Мекеменің АҚ сұрақтарына қатынасы байланысты болатын негізгі фактор оның өмір жасының деңгейі болып табылады. Осылайша, мысалы танымал талдаушы Gartner Group компаниясы мен Carnegie Mellon университеті компаниялардың өмір жасын анықтаудың моделін ұсынды. Өмір жасының әртүрлі деңгейлеріне АҚ саласындағы түрлі қажеттіліктер сәйкес келеді. Аталған модельдер келесі тарауларда толығырақ қарастырылады.

1.4.1 Gartner Group моделі

Gartner Group компаниялардың өмір жасының төрт деңгейін атап көрсетеді: нөлден бастап үшпен аяқтайды (1.1-кестені қараңыз).

1.1-кесте

АҚ тұрғысынан компаниялардың өмір жасының деңгейлері

Өмір жасының деңгейі	Компанияның АҚ режимін ұйымдастыру сипаты
0	Компанияның АҚ қамтамасыз ету қажеттілігі толық сезілмеген және мұндай тапсырма қойылмай отыр. Арнайы бөлінген АҚ қызметкерлері жоқ. Автоматтандыру қызметі дәстүрлі механизмдер мен TCP/IP протоколы стегінің ақпаратты қорғау және Intranet сервисінің, қосымшалар мен операциялық орта құралдарын пайдаланады (ОЖ, МББЖ, ERP, ERP II, CRM).
1	АҚ қамтамасыз ету мәселесі компанияны басқаруда техникалық деп қарастырылады. Арнайы ақпаратты қорғау қызметінің жоқтығы. АҚ қолдайтын ұжымдық шаралардың жоқтығы. Қаржыландыру IT-технологияда тек қана бюджет көлемінде жүзеге асады. Ақпаратты қорғау құралдарына қосымша 0 деңгейдегі автоматтандыру қызметі ақпаратты қосымша көшіру құралдарын, үзіліссіз электркүш құралдарды, желіаралық экрандарды, виртуалды бөлікті желіні, антивирустық құралдарды, мөлдір шифрлеу құралдарын және e-Token құралын тартуға мүмкіндік береді.
2	Компанияның АҚ қамтамасыз ету мәселесі түсінікті және өзара байланысқан ұйымдастырушылық және техникалық шаралар кешені қарастырылады. КАЖ қорғанысының минималды, базалық деңгейлеріне жауап беретін ақпараттық тәуекелдерді талдау әдістемелері енгізілген. Компанияда АҚ қызметінің құрамы мен құрылымы анықталған. Корпоративті АҚ саясаты қабылданған. Қаржыландыру АҚ корпоративті жүйесі үшін бөлек бюджет есебінде жүреді. АҚ қызметі 0 және 1 деңгейлерінің ақпаратты қорғау құралдарына қосымша рұқсатсыз кіру құралдардан қорғану құралын, басып кіруді анықтау жүйесін (IDS), ашық кілттер инфрақұрылымын (PKI), сонымен қатар компанияның қауіпсіздік саясатына сәйкес келетін ұйымдастырушылық шараларын (ішкі және сыртқы аудит, бизнесті үздіксіз енгізу және қорғау жоспарларын құру, аймақтан тыс оқиғалар болғандағы әрекеттер) тартады.
3	Компанияның АҚ қамтамасыз ету мәселесі толық түсінікті. Бизнес-мәдениетпен қоса, компанияның АҚ мәдениеті ұғымы да бар. Ақпараттық тәуекелдерді толық сандық талдау әдістемесі мен сәйкес құрылғылар да қолданылады. Аймақтық қызмет түрі – АҚ қызметінің директоры енгізілген (CISO). КАЖ қауіпсіздігінің ішкі аудит группасы (CISA), компьютерлік қылмыстарды зерттеу және алдын алу группасы, экономикалық қауіпсіздік группасының құрамы мен құрылымы анықталған. Компанияның басшылығымен қауіпсіздік концепциясы мен саясаты, қорғану жоспары мен басқа да нормативті-әдістемелік мәліметтер мен қызметтік жол сілтегіштер тұжырымдалған. Қаржыландыру арнайы бюджет көлемінде бөлінеді. АҚ қызметі 0 - 2 деңгейлерінің ақпаратты қорғау құралдарына қосымша компанияның АҚ орталықтандырылған басқару құралына және желілік ресурстар басқару платформасын интеграциялау құралына айналады.

1.4.2 Carnegie Mellon University моделі

Ақпараттық жүйе тұрғысынан компаниялардың өмір жасының деңгейін анықтау бойынша Carnegie Mellon университеті кеңейтілген модельді ұсынды:

Осы модель бойынша компанияның өмір жасының бес деңгейі қаралады. Оларға АҚ ұйымдастыру мәселелерін сәйкес қоюға болады (1.2-кестені қараңыз).

1.2-кесте

Компанияның өмір жасының деңгейін анықтау моделі

Мекеменің өмір жасы	Қасиеттері	АҚ саласында мекеменің сипаты
1. Анархия	Қызметкерлер ненің дұрыс, ненің бұрыс екенін өздері анықтайды. Шығындар мен сапа болжанбайды. Қалыптастырылған жоспар болмайды. Өзгерістерді бақылау болмайды. Жоғарғы басшылық жұмыстың нақты жағдайын дұрыс білмейді.	АҚ саласында саясат қалыптаспаған, басшылық бұл сұрақтармен айналыспайды. АҚ қамтамасыз етумен қызметкерлер өз ықыласы қойылған есепті түсінуі бойынша айналысады.
2. Фольклор	Ұйымдасқан үрдістердің белгілі бір ретпен қайталану уақыты анықталған. Ұйым тәжірибесі ұжымдық мифологиясын талдау арқылы көрсетілген. Білім жұмысшының жеке тәжірибесі түрінде жинақталып, олардың жұмыстан шығуы кезінде жойылады.	Басшылық деңгейінде ақпараттық қауіпсіздікті қамтамасыздандыру тапсырмалары жөнінде анықталған түсініктер кездеседі. Ақпараттық қауіпсіздікті қамтамасыздандырудың стихиялық процедуралары болады, олардың толықтығы және тиімділігі талданбайды. Процедуралар құжатталмаған және оған қатысатын жұмысшылармен тікелей байланысты. Басшылық тарапынан ақпаратты қорғау процедурасын құру жөнінде талаптар қойылмайды.
3. Стандарттар	Ұжымдық мифология қағазда жазылған. Үрдістер орындаушылардың жеке сапасына тәуелсіз қайталанып отырады. Тиімділікті өлшеуге арналған үрдістер туралы ақпарат жинақталмайды. Үрдістердің қалыптасқан анықтамаларының болуы, олар жұмыс істеп тұр деген сөз емес. Ұйым өзінің тәжірибесін бағытталған бизнеске бейімдей бастайды. Жете меңгерудің қажетті деңгейін анықтау мақсатымен жұмысшылардың біліміне, іскерлігіне талдау жүргізіледі. Жетік меңгерудің даму стратегиясы өңделеді.	Басшылық ақпаратты қауіпсіздендіру саласындағы тапсырмаларды қолдайды. Ұйымдар ақпараттарды қауіпсіздендіру политикасына қатысты құжаттарға ие. Басшылық ақпараттық қауіпсіздендіру және сәйкесінше құжаттарды тіркеу саласында стандарттарды қолдануға қызығушылық танытып отыр. Ақпараттық технологиялар тіршілік циклінің барлық сатыларындағы АҚ режимін басқару тапсырмалары қолдау көрсетілуде.

4. Өлшенілетін	Үрдістер өлшеніледі және стандартталған.	Ақпаратты қауіпсіздендіру режимін қамтамасыздандыру жөніндегі және қандай да бір сапа бойынша реттелген құжаттардың толық жинағы кездеседі. Қолданылыс тәртібі қадағаланып отырылады, құжаттар қызмет шеніндегілер әрекетіне қызмет етеді. АҚ саласындағы ішкі (кей жағдайда сыртқы да болуы мүмкін) аудит жүйелі түрде жүргізіліп отырылады. Басшылық ақпаратты қауіпсіздендіру саласындағы сұрақтарға аса назар аударуда, сонымен қатар көрсетілетін қызымдар деңгейіне және осал тұстарына, болуы мүмкін оқиғаларға қатысты потенциалды шығындарды ескереді.
5. Тиімділейтін	Белгілі бір ретпен қайталану, тиімділікті өлшеу, оптималдау фокусы. Үрдістерді функционалдау туралы барлық ақпараттар бекітіледі.	Басшылық кездесетін тәуекелділіктің сандық мөлшеріне қызығушылық танытуда, ақпаратты қорғау жүйесін құру жөнінде тиімді талаптар қойып, алдағы тәуекелдер деңгейін таңдауда өз жауапкершілігіне алуға дайын.

Дамудың әртүрлі деңгейіндегі ұйымдар үшін ақпараттық қауіпсіздендіру режимін қамтамасыздандыру мәселелері әртүрлі жолмен құрастырылып (анық емес түрде кездессе де), шешіледі.

Бірінші деңгейде мұндай мәселелер басшылық тарапынан заңды түрде ұсынылмайды. Әрине, бұл қызметкерлердің жеке қалауы, ынтасы бойынша шешілмейді деген сөз емес. Оған мысал ретінде келісідей жағдайды қарастыруға болады. Өрт шалу себебінен жалға алынып отырылған ғимараттың барлық есептеуіш техникалары мен мәліметтері жойылған, жарнамалық бизнеспен айналысатын кішігірім ұйым. Бірақ ол бір аптадан соң-ақ өз жұмысын қалыпқа келтіре алды. Өйткені кейбір қызметкерлер өздерінің қалауы бойынша маңызды ақпараттарды CD-ға сақтап қойды немесе олардың үй компьютерлерінде кейбір мәліметтер сақталуы, әртүрлі адреске электронды пошта арқылы жіберіліп, қайтарылуы талап етілген жағдайларда сақталынған мәліметтер болуы мүмкін. Нәтижесінде фирма жұмысының сәтті жалғасуына септігін тигізген бағалы ақпарат көзінің бірсыпырасын қалыпқа келтірдік (ал техниканы сатып алуға болады). Осыған дейін басшылық тарапынан ақпаратты қауіпсіздендіру мәселелері қойылған жоқ, алда да қойылмайды деген сенімдеміз. Нәтижесінде сәтті аяқталған мысалдардан өзге, ақпараттық қауіпсіздендіруді асыра қолдану нәтижесінде көп зардап әкелген кездер де кездеседі. Дегенмен ұйым басшылығының көзқарасы бойынша ақпараттық қауіпсізден-

діру режимін қамтамасыздандыру талаптары өзекті емес. Мұндай ұйымдар көбінесе өміршең келеді.

Екінші деңгейде ақпаратты қауіпсіздендіруді қамтамасыз ету мәселелері бірте-бірте пайда болатын тәжірибе нәтижесіне негізделе отырып, заңсыз түрде шешіледі. Шаралар кешені (ұжымдық және программалық-техникалық) потенциалды мүмкіндіктер ретінде ықтималдылығы мол қауіптерден сақтануға мүмкіндік туғызады. Қорғаныс тиімділігіне қатысты мәселелер туындамайды. Осылай, бірте-бірте толығып отыратын тәуекелдер класын ұйымдастыруға арналған заңсыз тізімдер қатары қалыптаса бастайды. Егер ешқандай маңызды оқиғалар туындамаса, онда ұйым басшылығы ақпаратты қауіпсіздендіру сұрақтарын басты, маңызды мәселе ретінде санамайды. Ал егер маңызды оқиғалар туындаған жағдайда, пайда болған қауіпсіздікті қамтамасыз ететін жүйе түзетіліп, кейбір жағдайда қорғаныста мүмкін болатын осал тұстарды іздеу қажеттілігі басшылық тарапынан қолдауға ие. Бұл жағдайда тәуекелді анықтау нұсқаларының бірі келесідей көрініске ие: осал тұстары, потенциалды бұзушылар және олардың мотивациялары (бұзушылар моделі), сондай-ақ анықталған осал тұстармен байланысты оқиғаның даму сценарийі де белгілі. Ұйымдар даму сатысының бұл деңгейінде тәуекелділікті талдау әдісінің жергілікті (өзге технологиялардың тіршілік циклі сатыларымен байланыс орнатылмаған) қойылымы типтік болып табылады: бұзушы моделін анықтап, нақты ақпараттық жүйелерге арналған өзекті тәуекелдер класын келтірсек жеткілікті. Ал контршара нұсқаларын талдау тапсырмалары, тәуекелді басқару тиімділігін қадағалау өзекті мәселе ретінде қарастырылмайды.

Үшінші деңгейде ұйымдарда ақпараттық қауіпсіздендірудің базалық деңгейімен қамтамасыз ететін сапалар мен ұсыныстар шараларына негізделген (мысалы, ISO 17799). Құжаттау мәселесі қадағалануы тиіс. Басшылық көзқарасы бойынша, тәуекелдерді талдау мәселесі дәл қазір шешуді талап етпейді. Оларды талдау барлық тіршілік цикл сатыларындағы ақпаратты қауіпсіздендіру режимін басқару технологияларының бір элементі ретінде қарастырылады. Тәуекел түсінігі ықтималдылық, қауіп, осалдылық және құндылық тәрізді аспектілерден тұрады. Бұл жағдайда тәуекелді (белгілі бір кластың) бағалау нұсқаларының бірі: нәтижесінде көрсетілген осал тұстар (белгілі бір кластың) қауіп туғызуға себепші болатын оқиғаның пайда болу ықтималдығы. Жалпы жағдайда ақпаратты қауіпсіздендіру режимін басқару технологиясы келесідей элементтерден тұрады:

- ақпаратты қауіпсіздендіру мақсатында ұйымдар ақпараттық жүйелерінің құжатталуы;
- ұйымды басқару мақсатымен ақпараттық ресурстардың категориялануы;

- ақпараттық технология қауіпсіздендіру саласында кездесетін түрлі оқиғаларға мүмкін болатын әсерлерді анықтау;

- тәуекелдерді талдау;

- барлық тіршілік цикл сатыларындағы тәуекелдерді басқару технологиясы;

- ақпаратты қауіпсіздендіру саласындағы аудит.

Ұйымдар дамуының бұл сатысында тәуекелдерді талдау ақпаратты қауіпсіздендіру режимін басқару технологиясының басқа компоненттерімен байланысты. Толығырақ бұл сұрақтар 3-бөлімде қарастырылған.

Төртінші деңгейде ұйым басшылықтары үшін ақпаратты қауіпсіздендіру режимін сипаттайтын параметрлерді өлшеу мәселелері өзекті болып болады. Басшылық бұл деңгейде қалдық тәуекелдердің (әрдайым қалып отыратын) анықталған шамасын таңдауға жауапты. Ереже бойынша, тәуекелдер бірнеше критерий бойынша бағаланады.

Ақпаратты қауіпсіздендіру режимін басқару технологиясы өзгеріссіз болады, бірақ тәуекелдерді талдау сатысында қалдық тәуекелдер өлшемдерін және тәуекелдерді басқару барысындағы контршара түрлі нұсқаларының тиімділігін бағалауға мүмкіндік туғызатын сандық әдістер қолданылады.

Бесінші деңгейде ақпаратты қауіпсіздендіру режимін қамтамасыздандыру саласында оптималдау мәселелерінің түрлі нұсқалары қарастырылады. Қойылымға мысал:

- ақпараттық қауіпсіздендіру ішкі жүйесінің, қалдық тәуекелдердің көрсетілген деңгейінде «құны-тиімділік» критериі бойынша оптималданған нұсқасын таңдау;

- қауіпсіздік ішкі жүйесінің белгіленген құны бойынша қалдық тәуекелдер минималданатын ақпараттық қауіпсіздендіру ішкі жүйесінің тиімді нұсқасын таңдау;

- ақпараттық қауіпсіздендіру ішкі жүйесінің қалдық тәуекелдердің орнатылған деңгейінде тіршілік циклін ең аз мөлшерде иелік ететін сәулетті таңдау.

II ТАРАУ

ХАЛЫҚАРАЛЫҚ СТАНДАРТТАРДЫ ЖӘНЕ ТӘУЕКЕЛДІЛІКТІ БАСҚАРУ

Соңғы жылдары технологиясы дамыған әртүрлі елдердің кәсіпорындарында ақпараттық қауіпсіздік(АҚ) режимінің тәжірибелік сұрақтарына арналған ақпарат қауіпсіздік стандарттарының жаңа буындары пайда болды. Бұл алдымен ақпарат қауіпсіздігінің бағалауы және оны басқаруының халықаралық, мемлекеттік стандарттары – ISO/IEC 15408, ISO/IEC 17799 (ISO/IEC 27002), BSI; ақпараттық қауіпсіздік сұрақтары көрсетілген аудит стандарттары - COBIT, SAC, COSO, SAS 55/78 және т.б.

Кез келген компанияның АҚ режимі жоғарыдағы стандарттарға сай келесілерден тұрады:

- Біріншіден, компаниядағы ақпарат қауіпсіздігін қамтамасыз ету мақсатын анықтау.
- Екіншіден, ақпарат қауіпсіздігімен эффективті басқару жүйесін құру.
- Үшіншіден, өтінген мақсаттары ақпарат қауіпсіздігіне сай бағалау үшін мөлшерленген және сапалы көрсеткіштердің бөлшектенген жиынтықтарын есептеу.
- Төртіншіден, ақпарат қауіпсіздігін қамтамасыз ету және оның ағымдағы жағдайын бағалау аспаптарын қолдану.
- Бесіншіден, тәуекел талдауының үрдісінде және істің ағымдағы жағдайын объективті бағалауға мүмкіндік беретін басқарулар әдістемесін (жүйелік критерийлер және ақпарат қауіпсіздігін қамтамасыз ету өлшемінің түсініктемесі) қолдану.

Көрсеткіштердің кешенді есебі егерде ережеге сай тексерілсе, корпоративті ақпараттық жүйе (КАЖ) ақпарат қауіпсіздігіне сәйкес техникалық бағдарламадан ғана тұрмайды, сонымен қатар басқару ұйымдары оның қамтамасыз ету шараларын бақылап, АҚ режим ұйымына кешенді әдістемесін ұсынады.

Ақпарат қауіпсіздігін басқару (Information Security Management) жүйесінің барлығы жекеленген тәуекелді ақпарат қауіпсіздігін басқару (Risk Management), кәсіпорындарда АҚ режим ұйымының міндетті шарттарын қанағаттандыру болып табылады. Көптеген шетелдік ұлттық институттардың стандарттары және ақпарат қауіпсіздігінің кешенді мәселелерін шешудегі мамандандырылған ұйымдар, ақпараттық тәуекелдерді (риск) басқару концепциясына ұқсастарын ұсынды. Әртүрлі мекемелермен басқа да ұйымдардағы АҚШ NIST стандарттарының қатары, сонымен қатар BS

7799 (ISO/IEC 27002) Британдық стандарттары, BSI, Германия стандартының тұжырымдамаларын қарастырамыз.

2.1 ISO 27002 халықаралық стандарты

1993 жылы Ұлыбританияның Сауда министрлігінің компанияларында және коммерциялық ұйымдардағы ақпараттық қауіпсіздіктің қамтамасыз етуінің тәжірибелік тұрғылары туралы оқу құралы жарияланды. Көптеген ұйымдарда оқу құралын администраторлар өте сәтті пайдалана бастады. Кейіннен бұл оқу құралының болжамын толықтырып, BS 7799 Британдық стандарты «Ақпарат қауіпсіздігінің практикалық ережесін басқару» (1995 ж.) ретінде қабылданды. Стандарт Ұлыбританияда ғана емес, басқа елдерде де ерікті түрде қолдана бастады. 1998 жылы ақпараттық қауіпсіздікті тексерудің сұрақтарына қатысты стандарттардың екінші бөлімі шықты. 2000 жылы BS 7799 стандартына негізделген халықаралық ISO/IEC 17799 стандарты қабылданды. 2002 жылдың қыркүйегінде ISO/IEC 17799 басты жағдайларының АҚ режим ұйымының талаптарына және қазіргі заманғы ақпарат технологияларының даму есебімен қайтадан толықтырылып қарастырылды. 2007 жылы ISO/IEC 17799 негізінде ISO/IEC 27002 стандарты құрылды. Қазіргі уақытта ұйымдар мен кәсіпорындарда ерікті түрде бұндай стандарттарды құжаттарда кеңінен пайдаланады, бірақ аудитке байланысты тарау жоқ (2 бөлім, BS 7799 аналогы). BS 7799, 2 бөлім аналогы 2005 жылы ISO/IEC 27001 стандарты ретінде шығарылды.

2.1.1 BS 7799 стандартына шолу

1-бөлім: Тәжірибелік ұсыныстар, 2000 жыл. АҚ режимінің ұйымы келесі тұрғыларды қарастырады:

- қауіпсіздік саясаты;
- қорғаныс ұйымы;
- ақпараттық ресурстар классификациясы және оларды басқару;
- дербес (персонал) басқару;
- физикалық қауіпсіздік;
- компьютерлік жүйелерді және желілерді басқару;
- жүйелерге рұқсатты (доступ) басқару;
- өңдеу және жүйені бақылап отыру;
- ұйымның үзіліссіз жұмысын жоспарлау;
- АҚ талаптарына жүйенің сәйкестігін тексеру.

2-бөлім: Спецификациялар, 2000 жыл. Сол тұрғыларға арналған, бірақ АҚ режим сертификациясының көзқарасымен стандарттар талаптарына сәйкестендірілген. ISO 27002 стандарттарының негізгі жағдайын қарастырамыз. Сонымен, Ұлыбританияның Ұлттық стандарттар институты ұсынған стандарттың әдістемелік схемасына сүйеніп, алдымен оның түпкі

мақсаттарын, стандарт жағдайының мәселесін қалыптастырамыз, содан кейін кәсіпорындағы АҚ басқару бойынша ұсыныстарды көрсетеміз.

1-бөлімше. АҚ саясаты

Мақсаты. Тапсырмаларды қалыптастыру және ұйым жетекшісі жағынан ақпарат қауіпсіздігі аймағынан қолдау мөлшерін қамтамасыз ету.

1-бөлім. Жоғарғы басқарушы ұйым қызметкерлерінің арасында қауіпсіздік саясатының таралуын, өзінің АҚ сұрақтарына қызығушылық пен қолдауын көрсету және алдына нақты мақсат қоюы қажет.

АҚ саясатына мазмұндалған құжат АҚ режимінің қамтамасыз етілуіне жауап беретін барлық қызметкерлерге рұқсат (доступен) болуы және келесі сұрақтарды қарастыруы қажет:

- АҚ анықтау;
- ұйым үшін үлкен мәні бар АҚ себептері;
- өлшеуге мүмкіндік беретін АҚ көрсеткіштері және мақсаттары.

2-бөлім. Қауіпсіздік саясатында арнайы формальдік талаптардың болмауына аса мән беріледі.

2-бөлімше. Қорғаныс ұйымы

2.1. АҚ инфрақұрылымы

1-бөлім. АҚ режимін қамтамасыз ету үшін ұйымдарды басқару құрылымына сай құру қажет. Қауіпсіздік режимін қолдануға бағытталған іс-әрекеттің координациясымен қорғанысты қамтамасыз ету бойынша бөлім міндеттерімен АҚ саясатының коррекциясына арналған басшылар жиналысын тұрақты өткізу тиіс. Мүмкіндігінше ақпаратты қорғау аймағы үшін мамандар кеңесшісін қатыстыру қажет. Қорғауды бұзатын жағдайларды қарастыруға және стандарттауға, сонымен қатар қазіргі заманғы тенденциялар хабардар болуы үшін басқа да ұйымдарға ұқсас мамандармен келісімшарттар құру ұсынылады.

АҚ мәселелерін кешенді бағытта жан-жақты рұқсат ету қажет, мысалы мәселелерді тиімді шешу мақсатында тексерушілердің, қолданушылардың және администраторлардың бірлескен жұмысы.

2-бөлім. Бағынышсыз тестілеу орындалуы тиіс. АҚ басқару жүйесімен айналыспайтын ішкі *ұйымдармен сыртқы тексерушілерге тестілеу өткізуі мүмкін.*

2.2 Ұйымның және басқа қолданушылардың (пользователей) рұқсатқа (доступ) қауіпсіздігін қамтамасыз ету

Мақсаты. Ұйымға бөтен қолданушылардың рұқсаты бар ақпараттық қорларды қауіпсіздікпен қамтамасыз ету.

1-бөлім. Бақылау құралдарының талаптарын анықтау үшін қорғанысты бұзушы тәуекелділік анализін өткізу тиіс. Бұл құралдар басқа ұйыммен келісімшартқа отырғанда өзара келісуі қажет.

2-*бөлім.* Келісім талаптарының анализімен олардың орындауын тексеру міндетті болып табылады.

3-бөлімше. Ресурстар классификациясы және оларды бақылау

3.1 Ресурстарға жауапкершілік

Мақсаты. Ұйым ресурстарын сенімді қорғаныспен қамтамасыз ету.

1-бөлім. Барлық негізгі ақпараттық ресурстарға жауап берушілер болуы тиіс.

Сонымен қатар қорғаныс шараларына байланысты жауаптыларды тағайындау қажет.

2-бөлім. Тексеруді өткізгенде төменде көрсетілген ресурс тізімін тексеру қажет:

– ресурс түрін, сериялық нөмірін;
– жауапты;
– құпиялық деңгейін;
– тұрған жерін;
– ақпарат таратушыны (носитель) (мәліметтер үшін);
– енгізу күнін және тексерісті бақылау.

3.2 Ақпараттар классификациясы

Мақсаты. Ақпараттық ресурстардың қорғау деңгейін сенімді қамтамасыз ету.

1-бөлім. АҚ аумағын қамтамасыз ету басымдылығын беру үшін критикалық категория бойынша ақпаратты классификациялау кіреді. Кейбір ақпараттардың түрлері қосымша қорғауларда немесе арнайы үндеулерде қолдана алады. Критикалық ақпарат категориялары қолданушыларға осы ақпаратпен арнайы үндесу қажеттіліктері туралы және оны қорғау деңгейін анықтауға мүмкіндік береді.

2-*бөлім.* Тексерушілер критикалық категориялар бойынша классификация жүйесінің толық әрі анық болуына, қызметкерлерге түсінікті және АҚ саясатына сәйкес келуіне сенімді болуы керек.

4-бөлімше. Қызметкерді басқару

4.1 Ресурстарға рұқсаты бойынша нұсқау қызметінің қауіпсіздік сұрақтары

Мақсаты. Қызметшілерге тәуекелділік қателіктерін, ұрлықтарды, алаяқтықты немесе ресурстарды заңсыз қолдануды азайту:

1-бөлім. Қауіпсіздікпен сабақтас тұрғылар қызметшілер жиыны кезеңінде олардың қызмет нұсқауында, келісімшартында, сонымен қоса берілген қызметкерге жұмыс уақыты әрдайым бақыланатыны туралы ескерткен жөн. Жетекшілерге берілген қауіпсіздік жауапкершілігінің қыз-

метіне барлық қызметтердің нұсқаулары көрсетілуі қажет. Егерде олар ақпарат сыншыларымен жұмыс істейтін болса, онда жұмысқа қабылдайтын тұлғаны міндетті түрде тексеру қажет. Ұйымның барлық қызметкерлерін және басқа ұйымдардың ақпараттық ресурстарын қолданушыларға конфиденция (таралмаған) туралы өзара келісуі қажет.

2-бөлім. Тексерушілерге критикалық маңызды ақпараттар рұқсатына байланысты кандидаттардың қызметі бойынша таңдау процедурасын және жұмысшы қызметінің нұсқауларын тексеру қажет.

4.2 Қолданушыларды үйрету

Мақсаты. Ұйым жүйесінің қауіпсіздігін нормалық функциялау үшін қажетті процедуралардың орындалуына, қорғаныстың мәніне және АҚ режимінің бұзылу қаупі туралы қолданушыларға таныстыру.

1-бөлім. Қолданушылар қорғаныс процедураларын және ақпарат ресурстарын дұрыс пайдалануды үйренуі тиіс. Сонымен қатар міндетті түрде қолданушылар рұқсатын (құқықтық және шектеулік) ресми және жазбаша түрде бекіту қажет.

2-бөлім. 1-бөлімдегі көрсетілген талаптардың міндетті түрде орындалғанын тексеру.

4.3 Қауіпсіздік қаупін жасыратын жағдайларды қадағалау

Мақсаты. АҚ режимінің бұзылуына нұқсан келтірушілерді азайту және инциденттердің қайталануына мүмкіндік бермеу.

1-бөлім. Әкімшілік каналдары бойынша нұсқаушы мәліметіне дейін АҚ режимінің бұзылуы туралы дереу жеткізу керек. Барлық қызметкерлерге әртүрлі инциденттердің (қауіпсіздіктің бұзылуы, қауіпсіздік қаупі) түрлері туралы ескерту процедурасымен таныстыру керек. Олар мұндай жағдайлар туралы тиісті қызмет орындарына хабарлауы қажет. Ұйымдарда қауіпсіздік режимін бұзатын қызметкерлерге тәртіп жазаларын салу туралы формальді процедура орнатуы тиіс.

2-бөлім. Тексерушілерге қызметкерлердің АҚ режимі бұзылғанда қандай шаралар қолданатыны жайлы тексеру қажет.

5-бөлімше. Физикалық қауіпсіздік

5.1 Қауіпсіздік зонасы

Мақсаты. Есептеу техникаларға және сервистерге рұқсат етілмеген рұқсат оның жұмысы бұзылғанда да араласуына тыйым салу.

1-бөлім. Ақпараттық жүйелердің критикалық маңызы немесе ұйым сервистерінің осал жері туралы ақпараттар қорғаныс орындарында орналасуы тиіс. Рұқсат етілмеген рұқсаттың тәуелділігін немесе қағаз құжаттамасының бұзылуын азайту үшін ақпарат таратушының жұмыс үстелін пайдалану ережесін орнату ұсынылады.

2-бөлім. Тексерушілерге рұқсаттамалық режимі бар қауіпсіздік зоналарында критикалық маңызды ресурстардың орналасқанына көз жеткізуі қажет.

5.2 Құрал-жабдықты қорғау

Мақсаты. Ұйымның үздіксіз жұмысында ресурстардың бұзылуын және жойылып кетуін тоқтату.

1-бөлім. Құрал-жабдықты физикалық қорғауды қамтамасыз ету үшін оның бұзылуына рұқсат бермеу керек. Құрал-жабдықтың орналасуымен оның утилизациясы туралы мәселелерге көңіл бөлу керек. Рұқсат етілмеген рұқсаттармен басқа да қауіптер үшін, сонымен қатар көмекші құрал-жабдықтар үшін арнайы іс-шаралар қажет, мысалы электрожабдықтау және кабельдік желі.

2-бөлім. Тексерушілерге техникалық қызмет көрсетуді, инфрақұрылымнан тұратын электрожабдықтау апаттарынан қорғауды және құрал-жабдықты физикалық қорғау жағдайларын тексеру керек. Ғимараттан тыс орналасқан құрал-жабдықты зерттегенде ерекше мән беріледі.

6-бөлімше. Ақпараттық жүйелерді басқару

6.1 Эксплуатация ережесі және олардың дұрыс орындалуын қадағалау

Мақсаты. Ақпараттық жүйелердің дұрыс және сенімді жұмыс істеуін қамтамасыз ету.

1-бөлім. Желілермен компьютерлерді функцияналды қамтамасыз етумен басқару процедураларының міндеттерін анықтау қажет. Бұлардың барлығы инциденттерде, процедураларда және нұсқауларда бекітілуі керек. Дұрыс емес немесе рұқсат етілмеген іс-әрекеттердің тәуекелділігін азайту үшін бөлімше міндеттерінің принциптерін қабылдау қажет.

2-бөлім. Тексерушілер құжаттау образының операцияларына қажетті эксплуатациялар, өңдеулер, бақылап отырулар, тестілеулер бойынша ережелердің барлығын тексеру қажет.

6.2 Ақпараттық жүйелерді жобалау және оларды қабылдау

Мақсаты. Ақпараттық жүйелердің тәуекелділік ақауларын азайту.

1-бөлім. Ресурстардың қол жетерлік және ақпараттық жүйелерді өңдеу талаптарына байланысты аралық жоспарлаумен, дайындықпен қамтамасыз етіледі. Жүйелердің қайта жүктеу (перегрузка) тәуекелділігін азайту үшін болашақтағы қажеттілік өңдеулерін бағалау қажет. Жаңа жүйелерге құжаттауларды қабылдауға дейін эксплуатациялық талаптардың орындалғанын тексеру тиіс. Бірнеше қосымшалардан құрылған сервис үшін авариялық режимге өту талаптарын өңдеу қажет.

2-бөлім. Тексерушілер ақпараттық жүйелерді қабылдау критериясын, оның өнімділік бағаларын және әрбір сервис бойынша жұмыстарды қалпына келтіру жоспарларын тексеру қажет.

6.3. Бағдарламалық қамтамасыз етуді зиян келтірушілерден қорғау

Мақсаты. Деректердің және бағдарламаның біртұтастығын қамтамасыз ету.

1-бөлім. Бағдарламалық қамтамасыз ету – зиян келтіретін жағдайлардың енгізуімен және сақтыққа байланысты қабылданған шаралармен жүзеге асырылады. Қазіргі уақытта рұқсат етілмеген модификация қарымқатынасы бойынша бағдарламалық қамтамасыз ету осалдықтарын пайдаланатын барлық зиян келтіретін бағдарламалар (“компьютер вирустары”, “желілік құрттар”, “троян аттары” және “логикалық бомбалар”) бар. Ақпараттық жүйелердің администраторлары, ақпараттық жүйеге зиян келтіретін бағдарламалық қамтамасыз етуді енгізуге және арнайы шараларды жүзеге асыруға мүмкіндік беруге дайын болуы керек. Дербес компьютерге компьютерлік вирустардың пайда болуына мүмкіндік бермеу шараларын қабылдау қажет.

2-бөлім. Тексерушілер бағдарламалық қамтамасыз етуді енгізуге зиян келтіретін процедуралармен қарастырылмаған адекватты шаралар қабылдаса, онда жұқтыру жағдайларының тіркелгенін және қажетті мөлшерде құжатталғанын тексеру қажет.

6.4 Жүйелерге қызмет көрсету

Мақсаты. Ақпараттық сервистердің біртұтастығын және рұқсаттылығын қамтамасыз ету.

1-бөлім. Сервистердің біртұтастығы және рұқсаттылығы кейбір қызметтік процедуралардың орындалуына мүмкіндік береді. Резервті көшіру, оқиғалармен жазылуды тіркеу, сонымен қатар құрал-жабдықты функциялау шарттарын бақылауды стандарт процедуралары ұйымдастыру қажет.

2-бөлім. Тексерушілер резервті көшіру процедурасын ұйым талаптарына сәйкес екенін, операторлар барлық қажетті операциялардың хаттамаларын енгізгені туралы және олардың ескіруі бойынша шаралардың қабылдағанына сенімді болуы тиіс.

6.5 Желіге әкімшілік ету

Мақсаты. Желідегі ақпараттардың қорғанысын қамтамасыз ету.

1-бөлім. Ұйым шектерінде орналасқан желілер қауіпсіздігін басқарудың барлық сегменттеріне ерекше назар аударуды талап етеді. Конфиденциялдық деректердің қорғанысы үшін арнайы шараларды қажет ететін желінің ашылуы бойынша беріледі.

2-бөлім. Тексерушілер ұйымдарда қолданылатын қорғаныс шараларын тексеруі керек.

6.6 Ақпарат тасушылардың қорғанысы

Мақсаты. Ақпараттық қорлардың бұзылуы және ұйымның үзіліссіз жұмыс істеуін сақтап қалу.

1-бөлім. Ақпарат тасушыны қадағалау және оның физикалық қорғанысын қамтамасыз ету керек. Рұқсат етілмеген рұқсаттарды, жүйелік құжаттардың бұзылуларын, енгізу/шығару деректерін және ақпарат тасушыларды (магнит лентасы, дискілер, касеталар) қорғау үшін процедураларды анықтау қажет.

2-бөлім. Тексерушілер ақпарат тасушының сақтау режимін, орнатылған бақылау процедураларын тексеру керек.

6.7 Бағдарламалық қамтамасыз етумен деректердің ауысуы

Мақсаты. Модификацияны жоғалтуды және рұқсат етілмеген деректерді пайдалануды тоқтату.

1-бөлім. Ұйымдар арасындағы бағдарламалармен деректердің алмасуы формальді келісім негізінде жүзеге асырылады. Тасымалдау кезінде процедуралармен стандарттар орнатылуы керек. Электрондық пошта хабарларымен және электрондық деректермен алмасуды пайдаланғанда қауіпсіздікті қамтамасыз етуге аса мән беріледі.

2-бөлім. Тексерушілер АҚ ішкі электрондық құжат айналымымен және электрондық деректерімен алмасуды қорғау шараларын тексеру қажет.

7-бөлімше. Рұқсатты басқару

7.1 Қызметтік ақпараттың рұқсаттын басқару

Мақсаты. Ақпараттың рұқсатын бақылауды қамтамасыз ету.

1-бөлім. Ұйымдарда ақпараттардың таралу ережесі және рұқсаттың шектеуі орнатылу керек. Жүйе сервистерін және жүйе деректерін ұйым талаптарына сәйкес бақылау қажет.

2-бөлім. Тексерушілер өндірістік қажеттілікке байланысты ақпараттарға орнатылған ережелерді тексеру керек.

7.2 Қолданушылар рұқсатын басқару

Мақсаты. Ақпараттық жүйеге рұқсат етілмеген рұқсатты сақтап қалу.

1-бөлім. Ақпараттық жүйелерге рұқсат құқығын беретін процестерді басқару үшін формальдік процедуралар қажет. Бұл процедуралар қолданушылардың бастапқы тіркеуінен бастап, есептеу жазбаларының жойылуына дейінгі өміршеңдік циклдердің барлық кезеңдерін қамтиды. Жүйелік бақылау амалдарына мүмкіндік беретін супер қолданушы құқығына ерекше мән беру қажет.

2-бөлім. Тексерушілер тіркеудің формальді процедураларын және процедуралармен орнатылған заттың жағдайын тексеру керек. Ерекше артықшылықтарын бақылау қажет.

7.3 Қолданушылардың міндеттері

Мақсаты. Қолданушылардың рұқсат етілмеген рұқсатын сақтап қалу.

1-бөлім. АҚ режимінің басты шарттары тіркелген қолданушылардың көмегі болып табылады. Қолданушылар өзінің рұқсатты бақылауын қамтамасыз ету қажет, әсіресе қолданушы құрал-жабдығын қорғау және парольді пайдалана алуы қажет.

2 бөлім. Тексерушілерге қолданушылардың білім міндеттерімен оны толығымен пайдалана алатыны туралы тексерулер жатады.

7.4 Желілер рұқсатын басқару

Мақсаты. Желіге қосылған сервистердің рұқсат етілмеген рұқсатын сақтап қалу.

1-бөлім. Басқа желілік сервистерден қорғау үшін желі сервистеріне қосылуын қадағалау керек. Бақылау амалдарының қатарына төмендегілер кіреді:

- желілермен сервистердің арасындағы интерфейстер;
- қолданушылармен құрал-жабдықтың жойылған аутентификациялық механизмдері;
- ақпараттық жүйелерге қолданушылардың рұқсатын бақылау.

2-бөлім. Тексерушілер қолданушылардың тек өзіне қажетті сервистерге ғана рұқсаты бар екеніне сенімді болуы тиіс. Егер маршрутизацияны басқару саясаты өткізілсе, оның іс жүзінде қалай талап етілетінін анықтау керек.

7.5 Компьютерлер рұқсатын басқару

Мақсаты. Компьютерлерге рұқсат етілмеген рұқсатты қалпына келтіру.

1-бөлім. Рұқсатты тек тіркелген қолданушыларға беру қажет. Көп қолданушылық жүйелер төмендегілерден құралады:

- қолданушылардың шын екенін, егер қажет болса қолданушының орналасқан жерін немесе терминалын тексеру;
- сәтті және сәтсіз кіріс талпыныстарын бекіту;
- сенімді парольдердің таңдауын қамтамасыз ететін парольдермен басқару жүйесін беру;
- қажет болса жұмыс сеанстарының ұзақтығына шектеу қою.

Қауіпсіздік режимі бұзылғанда жоғарғы тәуелділік жағдайында өте қатты және ұзақ тұрған рұқсатпен басқару жүйесі бар.

2-бөлім. Тексерушілер парольдік қорғау минимумын қолдану кезінде жалпы парольдік пайдаланудағы парольді алмастыру мерзімін және пароль құрылымын, ұзындығын тексеру қажет. Рұқсат етілмеген рұқсат талпыныстары туралы сингнализация жүйелерін біріктіру үшін идентификация терминалдарының механизмдері бақыланады.

7.6 Қосымшалар рұқсатын басқару

Мақсаты. Ақпараттық жүйелерде сақталған рұқсат етілмеген ақпараттарға рұқсатын тоқтату.

1-бөлім. Қолданбалы жүйелердің рұқсатын басқару үшін логикалық рұқсатты бақылау амалының деректері қажет. Тіркелген қолданушылар бағдарламаларға және деректерге рұқсат беру керек. Қолданбалы жүйелер келесіні қарастырады:

- ұйымдарда қабылданған рұқсатты басқару саясатына сәйкес қосымшаларға және қолданушыларға рұқсатын бақылау;
- жүйелік бақылау амалын рұқсат етілмеген утилит рұқсатынан қорғауды қамтамасыз ету;
- ақпараттық ресурстарды бөлетін басқа жүйелерден қорғауын бұзбау.

2-бөлім. Тексерушілер рұқсатқа сәйкес шектеулерін тексеруі керек.

7.7 Жүйелерге және оны пайдалануға рұқсатын қадағалау

Мақсаты. Рұқсат етілмеген іс-қимылдарды анықтау.

1-бөлім. Ағымдағы жүйелерге бақылау өткізу рұқсатының саясатын басқару қалай орындалғанын анықтау қажет. Бұлар барлығы тәжірибеге сәйкес рұқсат саясатын бақылауды құру және қабылданған шаралардың эффективтілігін анықтау үшін қажет.

2-бөлім. Тексерушілерге рұқсатты басқару саясаты тәжірибеге жауап беретініне сенімді болуы керек.

8-бөлімше. Ақпараттық жүйелерді өңдеу және бақылау

8.1 АҚ жүйелерінің талаптары

Мақсаты. Ақпараттық жүйелерді қорғау амалдарының құрылуын қамтамасыз ету.

1-бөлім. Ақпараттық жүйелердің өңдеуіне дейін қауіпсіздікке қойылатын талаптардың сипатталуы және келісуі керек. Егер қорғау амалдары жобалауда және тапсырма талаптарының кезеңдерінде құрылса, онда олар көбінесе тиімді әрі арзан болып келеді. Қауіпсіздікке қойылатын барлық талаптармен ақпараттық өңдеуінің жалғасына арналған авария режимге өту қажеттілігімен қоса, ақпараттық жүйелерді құру бойынша жұмыстың жалпы жоспарын құжаттау және жоба талаптарын формалау кезеңдерін анықтау қажет.

2-бөлім. Тексерушілер қауіпсіздік сұрақтары талданғанда жобалау сатылары жүргізілгеніне көз жеткізу керек.

8.2 Қолданбалы жүйелердегі АҚ қамтамасыз ету амалдары

Мақсаты. Қолданбалы жүйелерде рұқсат етілмеген деректерді қолдануға, модификациялауға және жоғалтуға мүмкіндік бермеу. Қолданбалы жүйелерді жобалағанда оның қауіпсіздігін басқару, сонымен қатар аудитпен хаттамалау амалдарын құру қажет.

1-бөлім. Жүйелерді жобалау және пайдалану қорғаушылықтың негізгі базалық деңгейінің стандарттарына сәйкес келуі керек. Жүйелер бағалы немесе ұйымның критикалық маңызды ақпараттық ресурстарын, сонымен қатар оның қажеттілігіне байланысты қарама-қайшылық шараларын қабылдай алады. Мұндай шараларды идентификациялық қауіптерді есептеу қауіпсіздігі бойынша мамандар ұсыныстарына сүйене отырып, реализацияның іске асу мүмкіндіктерін анықтайтын шаралар.

2-бөлім. Тексерушілерге деректерді енгізгенде базалық қорғаныс деңгейлерін қамтамасыз ету үшін хабарламалардың шын екенін тексеретін механизмдерді қолданып, ақпараттың құпия сатыларын шифрлауды пайдаланған жөн.

8.3 Файлдарды қорғау

Мақсаты. Ақпараттық жүйені қолдауда және құрғанда ақпараттық қауіпсіздікті қамтамасыз ету**.**

1-бөлім. Жүйелік файл рұқсатына бақылау қажет. Бағдарламалық қамтамасыз ету немесе берілген қолданбалы жүйелерден құралған топтарды өңдеу және қолданбалы жүйелердің біртұтастығын қолдау міндеті болып саналады.

2-бөлім. Тексерушілерге бағдарламалық қамтамасыз етудің (БҚЕ) жұмыстық версиясы қалай сақталатыны, құрылатыны және жаңа версияның қалай тестіленетіні туралы түсіндіру қажет.

8.4 Эксплуатациялық және құру орталығындағы қауіпсіздік

Мақсаты. Қолданбалы БҚЕ және деректердің ақпараттық қауіпсіздігін қамтамасыз ету.

1-бөлім. Эксплуатациялық және құру орталығын қатаң бақылау қажет. Қолданбалы жүйеге жауап беретін басқарушылар жүйеге өзгертулер енгізгенде эксплуатациялық және құру орталығының қауіпсіздігінің бұзылмауын қадағалап отыру тиіс.

2-бөлім. Тексерушілердің барлық өміршеңдік этаптарын нақты бақылау процедураларын да тексеру қажет.

9-бөлімше. Ұйымның үздіксіз жұмыс істеуін жоспарлау

9.1 Ұйымның үздіксіз жұмыс істеуін жоспарлау сұрақтары

Мақсаты. Ұйымның үздіксіз жұмыс істеуін жүзеге асыру үшін жоспарлар құру.

1-бөлім. Өндірістегі критикалық маңызды процестерді ірі аварияларданжәне қиыншылықтардан қорғау үшін ұйымның үздіксіз жұмысын қамтамасыз ету жоспарлары талап етіледі. Өндірістегі критикалық маңызы бар процестермен сервистерді тез қайта қалпына келтіру үшін жоспарлардың реализациясы және процестің өңдеушісі болу қажет. Үздіксіз жұмыстың процесін жоспарлағанда сервистерде негізгі өндірістік процестерді жылдам қалпына келтіру, қауіп реализациясының ликвидициялық тәуелділігін азайту және идентификация сияқты іс-шаралардан тұрады.

2-бөлім. Тексерушілерге ұйымның үздіксіз жұмыс істеуін қамтамасыз ету жоспарымен және олардың реализациялық тәжірибесінің жалпы принциптерін тексеру қажет.

10-бөлімше. АҚ талаптарына сай жүйелерді тексеру

10.1 Жұмыс істейтін заң шығарушылардың талаптарын орындау

Мақсаты. АҚ режимінен тұратын заң беруші талаптарынан және келісім міндеттерін бұзудан қашу.

1-бөлім. Ақпараттық жүйелердің эксплуатациясын өңдегенде қауіпсіздіктің келісім талаптарымен құқықтары ескерілуі тиіс. Оны ресми түрде құжаттау қажет. Бақылауды таңдаған амалдарға да оның қатысы бар.

2-бөлім. Тексерушілердің маңызды шараларының құжаттары жеке ақпараттарды қорғау бойынша заң берушілердің нормасымен орындалуын қадағалау қажет.

10.2 Қауіпсіздік саясатына байланысты АҚ режимін тексеру

Мақсаты. АҚ саясатының режиміне және ұйым қауіпсіздігінің стандарттарына байланысты қамтамасыз ету.

1-бөлім. АҚ режимінің жағдайы тұрақты тексеруді талап етеді.

АҚ режимі декланарланған қауіпсіздік саясатына және қауіпсіздікті қамтамасыз етудің қабылданған стандарттарына жауап береді.

2-бөлім. Қауіпсіздік қызметінің барлық қарым-қатынасы және оның қауіпсіздік саясатына байланысты сатылары тұрақты бақыланады.

10.3 Тестілеу кезіндегі қауіпсіздік шаралары

Мақсаты. Штат жұмысындағы тестілеу іс-әрекеті және тестілеу процесіндегі кедергілерді азайту.

1-бөлім. Тестілеу жүйелерімен жұмыс қорғанысы үшін амалдары болуы қажет.

2-бөлім. Тексерушілер тестілеу жоспарының атауын және ұйымдағы тестілеудің құрал-жабдық амалдарына рұқсатын тексереді.

2.1.2 BS 7799 (ISO 17799) стандарттарының дамуы

Британдық институты BSI стандарттары әртүрлі сұрақтарға арналған тәжірибелік кепілдемелер серияларын шығарды: тәуелділікті басқарумен бағалауға, АҚ режимінің аудитіне, BS 7799 стандартына байланысты қызметшінің жұмыс ұйымы. Бұл серия халықаралық ISO 17799 (ISO 27002) стандартын толықтырады.

2002 жылдың қыркүйегінде BS 7799 стандарты қайта қарастырылды. Оның жаңа нұсқасында: оқуға, бастапқы процедура интеграциясына, корпоративті жүйелердің ақпараттық технологияларының АҚ механизміне, сонымен қатар тәуекелділікті бағалаудың даму технологиясымен оны басқару сұрақтарына ерекше мән берілген. Мамандар пікірі бойынша бұл стандарттардың жаңаруы тек АҚ жаңа дәстүрін құру емес, сонымен қатар әртүрлі мемлекеттік құрылымдардың іс-әрекетін және ақпаратты қорғау аймағында халықаралық бизнес басшыларын координаттауға мүмкіндік береді.

2.2 BSI Германиялық стандарты

1998 жылы Германияда "Қорғаныстың базалық деңгейі үшін ақпараттық технологиялардың қорғанысы бойынша басшылық" шықты [3, 4]. Ол көлемі 4 Мб тұратын гипермәтіндік анықтаманы ұсынады (HTML пішімінде). Жалпы құжаттардың құрылымы 2.1-суретте көрсетілген.

Бұл құжаттар келесі блоктардан тұрады:

– АҚ басқару методологиясы (АҚ аймағындағы менеджментті ұйымдастыру, басшылық пайдаланатын методология):

– Ақпараттық технологиялардың компоненттері:

- негізгі компоненттер (АҚ ұйымдастыру деңгейі, процедуралық деңгей, деректерді қорғау ұйымы, төтенше жағдайдағы іс-әрекетті жоспарлау);
- инфрақұрылым (ғимарат, бөлме, кабельдік желі, жойылған рұқсатты ұйымдастыру);
- әртүрлі типтердің клиенттік компоненттері (DOS, Windows, UNIX, мобильдік компоненттер, басқа типтер);
- әртүрлі типтердің желілері («нүкте-нүкте» біріктіру, Novell NetWare желісі, ОЖ UNIX және Windows желісі, әр текті желілер);
- деректерді беру жүйесінің элементтері (электрондық пошта, модемдар, желі аралық экрандар және т.б.);
- телекоммуникациялар (факстер, автожауап бергіштер, ISDN базасындағы интегралданған жүйе, басқа да телекоммуникациялық жүйелер);

• БҚЕ стандарттары ;
• деректер қоры.

– Қауіпсіздік қаупі және шараларды бақылаушы каталогтары (әрбір каталогта 600 шақты атаулар бар).

Барлық каталогтар төмендегілерден құралады.

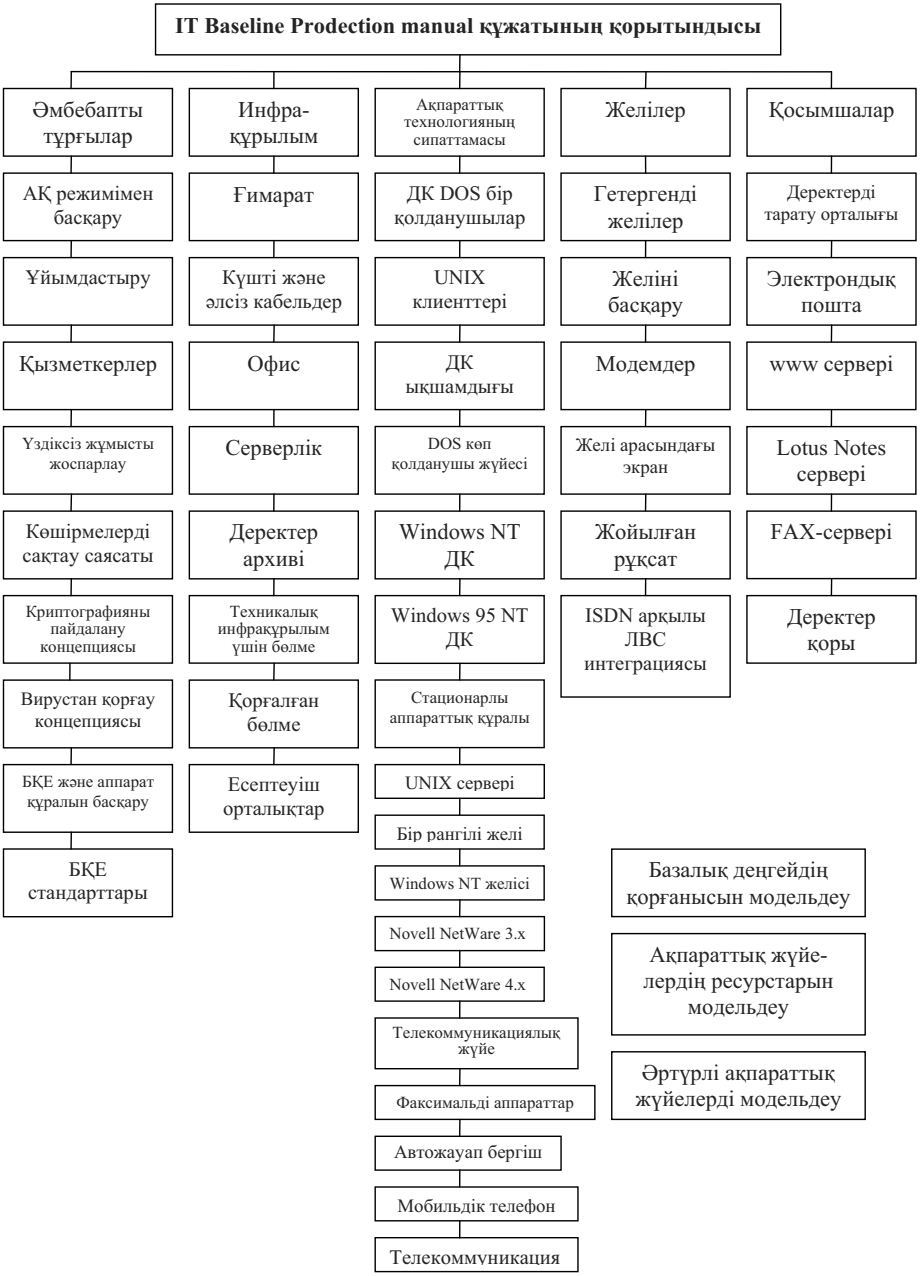
Кластар бойынша қауіптерге:

– форс-мажорлық жағдай;
– ұйымдастырушылық шаралардың кемшіліктері;
– адамның қателігі;
– техникалық ақаулар;
– қасақана іс-әрекеттер.

Кластар бойынша шараларды бақылаушыларға:

– инфрақұрылымның жақсаруы;
– шараларды бақылаушылар әкімшілігі;
– процедуралық шараларды бақылаушылар;
– техника-бағдарламалы шараларды бақылаушы;
– коммуникация осалдығын азайту;
– төтенше жағдайдағы іс-әрекеттерді жоспарлау.

Барлық компоненттер қандай да болмасын жоспарлармен қарастыралады: жалпы сипаттамалар, қауіпсіздік қаупінің сахналық ықтималы (қауіпсіздік қаупінің каталогынан берілген қауіптің компоненттеріне қолданылатындар тізбеленеді), шараларды бақылаушылар ықтималы (шараларды бақылаушылар каталогынан шараларды бақылаушылар ықтималы тізбеленеді). Шындығында, АҚ көзқарасы бойынша ақпараттық технологияның тараған компоненттері және оның спецификациясы максимальды ескергенде орындалады. Жаңа компоненттерінің шаралары бойынша стандарттарды жаңарту және оперативті толықтыру ұсынылады. Бұл ақпараттық ресурстарға лайықты назарды қажет етеді. 600 позициядан құрылған қауіпсіздік қаупінің және шараларды бақылаушылардың каталогтары толығымен жалпылама рұқсаты болып табылады. Ақпарат қауіпсіздігінің аудитінде, тәуекелділікті басқарғанда және тәуекелділік анализінің методикасын өңдегенде өз бетімен қолдана алады. Каталогтарға шолу (позиция атауы) 4-қосымшада көрсетілген.



2.2-сурет. BSI Германия стандарты. Құжаттың жалпы құрылымы

2.3 ISO 27002 және BSI 7799 стандарттарын салыстыру

ISO 27002 (BS 7799) [2] стандарттары ақпараттық зерттеулер технологиясының қолданылатын жалпы принциптерін жариялайды. Екінші бөлімде жарияланатын принциптердің орындалғанына мүмкіндік беретін формальдік процедураларда стандарттарға байланысты ақпараттық жүйелердің сертификациясына ерекше мән беріледі. Екі бөлімде де стандарттың көлемі 120 беттен аспайды.

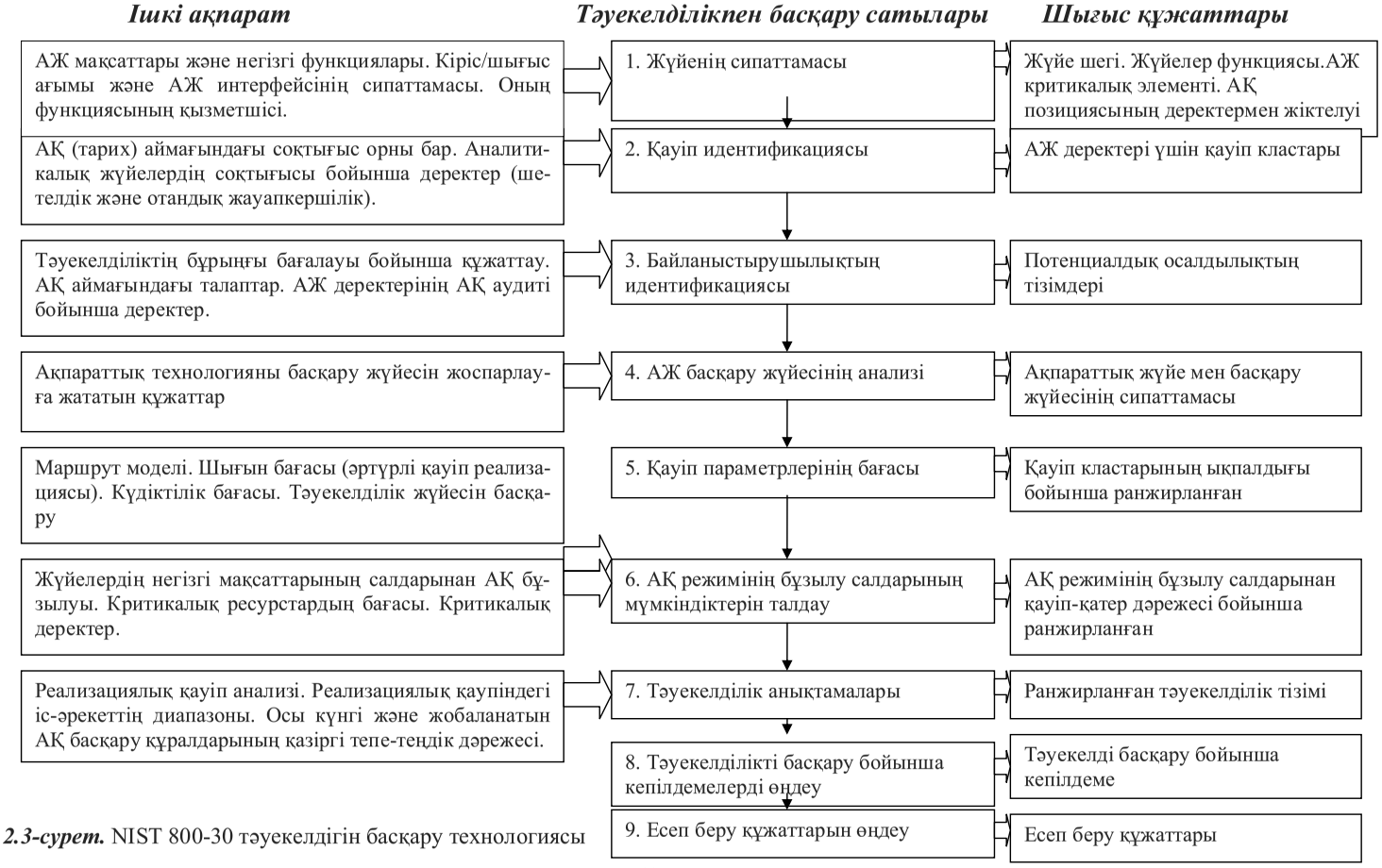
BSI германдық стандартында керісінше әртүрлі ақпараттық технология элементтері «жеке жағдайда» көп талқыланады. Құжаттың көлемі бірнеше мың беттерге өсе алады. Мұндай тұрғылардың қасиеттері және кемшіліктері болады. Оның қасиетіне әртүрлі элементтердің спецификасы кіреді. Британдық стандартпен салыстырғанда, қазіргі заманғы желілерде АҚ қамтамасыз ету ерекшеліктері анағұрлым жақсы қарастырылған. Басқа қасиеттері, стандарттар бөлімінің арасындағы байланысты түзетуге және тікелей өзгерулер енгізуге мүмкіндік беретін құжаттың гипермәтіндік құрылымы болып табылады. Стандарттың соңғы болжамы әрдайым Internetке рұқсатты. Қазіргі заманғы ақпараттық технологиялар бірыңғай нақтыланған деңгейлерді сақтайтындар үшін кемшілікпен мүмкін еместік. Жалпы элементтердің кең тараған түрлерін жазғанда «Басқалары» бөлімін енгізуге тура келеді.

Британдық стандартқа келсек, оның кемшілігі стандарттар талабына сәйкес тексерулерді жүзеге асыратын мамандар классификациясының жоғарғы талаптары болып табылады. Сонымен қатар онда қазіргі заманда кең тараған спецификалар толығымен қарастырылмайды

2.4 NIST 800-30 АҚШ стандарты

Берілген стандарт [5] ақпараттық тәуекелділікті басқару сұрақтарын толығымен қарастырады. Ұйымның тәуекелділігін басқару жүйесі ақпараттық технологиялардың пайдалануына байланысты келеңсіз жағдайларды және кәсіпорындардағы бизнес-мақсат негізінің орындалуын қамтамасыз етуді азайту керек.

Тәуекелділікті басқару жүйесі үшін компаниялардың ақпараттық технологияларының өміршеңдік циклінің басқару жүйесі жинақталады (2.2-кестені қараңыз).



2.3-сурет. NIST 800-30 тәуекелдігін басқару технологиясы

2.2-кесте

Ақпарат технологияларының әртүрлі өміршеңдік цикл сатысындағы тәуекелді басқару

Ақпараттық технологиялардың өміршеңдік циклінің фазасы	Тәуекелді басқарудың фазаларға сәйкестігі
1. Жоба алдындағы сатылар (берілген АЖ концепциясы: мақсаттар мен тапсырмаларды анықтау және оларды құжаттау)	АЖ деректері үшін АҚ қамтамасыз ету концепциясы, ағатын мақсаттар мен тапсырмалардың негізгі тәуекелділік кластарын шығару
2. АЖ жобалау	АЖ деректері үшін спецификалық тәуекелділікті шығару
3. АЖ құру: элементтерді қою, монтаж, түзету және конфигурациялау	АЖ функциялағанға дейін тәуекелділіктің барлық кластарының назарға қабылдануы және теңесуі қажет
4. АЖ функциялау	Тәуекелділіктің қайта бағалануы АЖ конфигурациясымен, ішкі шарттардың өзгеруімен байланысты болады
5. АЖ функциялануын тоқтату (есептеуіш және ақпараттық ресурстардың тағайындалуы бойынша қолданылмағандағы утилизациялануы)	Енгізілетін ақпарат ресурстарының қарымқатынасы бойынша ақпарат қауіпсіздігінің талаптарын орындау

NIST 800-30 стандартына келісетін негізгі сатылар тәуекелділікті басқару технологияларынан тұрады, 2.3-суретте көрсетілген.

Бұл ақпараттық тәуекелділікті басқару технологиясын кейінірек қарастырамыз.

2.4.1 Ақпараттық жүйенің алгоритмдік сипаттамасы

Берілген қадамда ақпарат жүйелерін құру мақсаты, оның шектері, АҚ аймағындағы талаптар және АҚ режимімен қоса ақпарат жүйелерін басқару компоненттері жазылады.

Сипаттама келесі жоспармен жүзеге асырылады:

– АЖ апппараттық құралы, оның конфигурациясы;

– Қолданылатын БҚЕ;

– Ақпарат технологияларының позициялық интерфейстері және жүйелері, яғни ішкі және сыртқы;

– Деректер мен ақпараттар типтері;

– АЖ деректерінің (міндеттері) жұмыс істейтін қызметкерлері;

– АЖ деректерінің (негізгі мақсаты) міндеттері;

– Ақпараттық процестер және критикалық деректер типі;

– АЖ функцияналды талаптары;

– Қызмет көрсететін қызметкерлердің және жүйені қолданушылардың категориясы;

– АЖ деректерінде пайдаланылған АҚ аймағындағы формальді талаптар (заңнама, тізімдемелік стандарттар және т.б.);

– АҚ бағыныңқы жүйесінің архитектурасы;

– Локальді желінің топологиясы;

– АҚ техника–бағдарламасын қамтамасыз ету амалы;

– Деректердің шығыс және кіріс ағымдары;

– АЖ деректерін басқару жүйесі (қызметтік нұсқаулар, АҚ сферасында қамтамасыз етуді жоспарлау жүйесі);

– АҚ аймағындағы бар басқару жүйелері (резервті көшіру, штатты емес жағдайдағы әсер ету процедуралары АҚ бойынша режимді бақылау және т.б.);

– Физикалық қауіпсіздік ұйымы;

– АЖ орталығының қарым-қатынасы бойынша бақылау және басқару (климатикалық параметрлермен, электроқыздырғышпен, толтырудан қорғау (защитой от затоплений), агрессиялық орталық және т.б.).

Жобалауға арналған сатылармен сипаттама мінезінің жүйелері үшін жауап беру дәрежесі әртүрлі болады. Бірінші жағдайда (жобалау сатылары) АҚ аймағында жалпы талаптар толығымен көрсетілген.

Жүйелерді сипаттау технологиясы

Тәжірибеде көрсетілген пунктілер бойынша ақпарат алу үшін төмендегілерді қолданған жөн:

– әртүрлі басқарушы және қызмет көрсетуші қызметкерлер топтарына арналған әр қилы сұрақшылар (check-беттер);

– қызметкермен ресми емес әңгімелер жүргізетін аналитиктер сұхбаты және содан кейін сипаттама туралы әңгімелеседі;

– формальді құжаттармен кәсіпорын құжаттамаларының анализі;

– мамандандырылған инструментариялар бағдарламасын қамтамасыз ету (БҚЕ). Сипаттама процесін автоматтандыруға мүмкіндік беретін әртүрлі бағдарламаны қамтамасыз ету (БҚЕ) бар. Оларға ақпараттық жүйелердің схемасын құруға мүмкіндік беретін әртүрлі сканерлер, есеп беру формаларын құруға мүмкіндік беретін ақпараттық жүйелердің құрылымын сипаттау үшін бағдарламалар кіреді (4-тарауда сипатталған).

2.4.2 Қауіптермен осалдықтардың идентификаторы

Берілген қадамда қауіптер идентификацияланады. Негізгі түсініктер:

– қауіп көзі – қауіп реализациясына әкелетін жағдайлар мен тәсілдер (шешімінде осалдылық потенциалын пайдалану);

– қауіп-қатер көзінің реализациясына әкелетін потенциал (немесе шара);

– осалдылық – қорғаныста әлсіз.

Қауіп тәсілінің бірі модель бұзушыларды құру болып табылады (2.3-кестені қараңыз).

2.3-кесте

Модель бұзушы мысалдары

Қауіп көзі	Мотивация	Қауіп реализациясының шешімі (сценалар)
Хакер	Бұзақылық, өзін-өзі таныту	ОЖ осалдығымен қолданылатын АЖ авторлық емес құқығы (сценария сипаттамасы)
Криминалдық құрылым	Финанс ақпаратын алу	Конфеденциалдық деректерді алу мақсатымен АЖ жетілдіру (сценария сипаттамасы)

Қауіп тізбегін құрғанда және оның деңгейін бағалағанда әртүрлі ұйымдардың қауіп кластарының тізіміне және деректер қаупінің реализация ықпалдылық мәндерінің рейтингілігі туралы хабарлау қажет. Ол тізімдер бірнеше ұйымдардың өзекті жағдайынан құрылады:

The Federal Computer Incident Response Center (FedCIRC), Federal Bureau of Investigation's National Infrastructure Protection Center, Security-Focus және басқалары.

3 және 4-тарауларда қауіп деңгейлерін бағалау үшін технологиялар және инструментариялар қарастырылады.

Осалдылықтарды идентификациялау

Шешімінде берілген қадамды орындау АЖ потенциалдық тізімінде және оның реализациясының маңызды шешімінде құрылады. Бір тәсілі кесте түрінде көрсетілген (2.4-кестені қараңыз).

2.4-кесте

Осалдылықтарды идентификациялау

Осалдылықтар	Қауіп көзі	Қауіп реализациясының шешімі (сценалар)
Желі аралық экранTelnet хаттамасы бойынша А серверіне және қонақ режиміне (ID = guest) рұқсаттар береді.	Сырттағы қолданушылар авторланбаған.	Осалдылық хаттамасын пайдаланғанда А сервері файлдық жүйеге рұқсат болуы мүмкін (сценария сипаттамасы) .
Компаниядан кететін қызметкерлердің тіркеу жазбалары 1-2 күн кешіксе, АЖ жойылады.	Ішкі бұзушылар жұмыстан шыққандармен бір қатынаста болуы мүмкін.	Операциялардың заңсыз финанстары (сценария сипаттамасы)

Тізім құрғанда АЖ сәйкесі үшін тәуелділік анализінің мамандандырылған әдістеріне, қоры әртүрлі ұйымдардың осалдылық каталогтарына (мысалы, АҚШ **(NIST)** институттарының стандарттары бойынша деректер қоры), осалдылықтың желілік сканерлеріне сүйенеді. Осалдылық деңгейін бағалағанда соқтығыс орны бар анализдің шешімдері, ішкі аудит деректері, ақпарат қауіпсіздігін қамтамасыз ету режимінің әдістері және қазіргі күнгі процедуралар қабылданады.

Егер АЖ жобалау сатысында болса, онда ақпаратты қорғау өндірушілерінің осалдылық құралдары бойынша статистикасы және АҚ жобаланатын процедураларын қамтамасыз етуі есепке алынады.

2.4.3 Ақпаратты қорғау ұйымы

Ұйым ықпалын басқаратын тізімдерді форматтау

Ақпаратты қорғаудың кешенді қамтамасыз ету режимінде қабылданған, модельге сәйкес жауапкершілік аймағы немесе деңгейі бойынша басқарушы ықтималдығының тізімдері құрылады (2.5-кестені қараңыз).

2.5-кесте

АҚ басқару

Деңгей	Қауіпсіздіктің критерияларымен ықпалын басқаратын кластар
Ұйымдастырылған деңгей	- әртүрлі жауапкершіліктер; - АҚ аймағында басқару жүйесінің мерзімдігін қайта қарастыру; - АҚ аймағында инциденттерді талқылау және хаттамалау; - тәуекелді бағалау; - АҚ аймағында үйрету; - АЖ автоматтандыру процедурасы және есептеу жазбасының жойылуы; - АҚ қамтамасыз ету жоспарының өзекті жағдайларда болуы
Процедуралық деңгей	Жекешелендірілген АҚ режимінен тұратын қамтамасыз ету ережелері: - ақпаратты тасушыға рұқсат; - АЖ жұмыс істейтін қызметкерлерді бақылау - климатикалық құрулармен күштік желілердің жұмыс сапасын қамтамасыз ету; - АЖ түскен деректерді бақылау
Техника-бағдарламалық деңгей	Техника-бағдарламалық деңгейді қорғаудың кешенді шаралары: - белсенді аудит және әсер етуші жүйе; - идентификация және аутентификация; - криптографиялық қорғаныс; - рөлдік модельдің рұқсатын орындау; - желілік құрал-жабдықтың жұмыс режимін бақылау

Әртүрлі басшылықта басқа да басқару құралдары толығырақ сипатталады, мысалы NIST SP 800-26-да.

АЖ басқару жүйелерін талдау

Келесі қадамдағы анықталатын қауіп параметрлері АЖ басқару жүйесінің ұйымдарына байланысты. Берілген қадамда осалдылық пен ықпалдылық іс-әрекетінің кейбір позицияларының басқару жүйесі талқыланады.

Әдетте басқару тәсілдерінің екі категориясы қарастырылады: техникалық және техникалық емес деңгейлер.

Техникалық деңгейдің тәсілдері келесі бөлімдерден тұрады:

– базалық деңгейдің талаптарын қамтамасыз ету (идентификация, кілттік жүйенің таралуын басқару, әкімшіліктендіру, қорғау жүйелерінің элементтер тәсілдері және БКЕ);

– бекітетін шаралар (аутентификация, авторлықтандыру, тоқтаусыз қамтамасыз ету, конфиденциялдық транзакциялар);

– АҚ аймағындағы бұзушылықтарды табу (аудит, басып шығудың әсері, антивирустық қорғаныс, БКЕ және деректердің біртұтастығын тексеру).

Техникалық емес деңгейдің тәсілдері – көптеген процедуралық және ұйымдастырушылық мінезінің басқару тәсілдері.

Тәуекелді параметрлерді бағалау үшін шкалалар таңдау

Тәуекелді параметрлерін бағалауда инцидентке әкелетін потенциалдық осалдылықты жүзеге асыратын ықпалдылықтар анықтамаларымен түсіндіріледі.

Типтік (көбірек таралған) шкалаларға бірнеше басқыштаулармен сапалы (балдық) шкалалар жатады, мысалы төменгі, орташа және жоғарғы деңгей. Бағалаулар объектілік факторларының есептеу сарапшысымен орындалады. Тәукелділік деңгейлері 2.6-кесте сияқты құрылады.

2.6- кесте

Тәуекелді баға үшін сапалы шкалалар мысалы

Тәуелділік деңгейі	Анықтамалары
Жоғарғы	Қауіп негізінде осалдылықтың тиімділік тәсілдерін азайтуға мүмкіндік беретін өте жоғарғы мотивация деңгейі бар
Орташа	Қауіп (бұзушы) негізінде осалдылықты азайтатын әдістердің төтенше тиімділігінде қолданылатын өте жоғарғы мотивация деңгейі бар
Төменгі	Қауіп (бұзушы) негізінде осалдылықты азайтатын әдістердің төтенше тиімділігінде қолданылатын төменгі мотивация деңгейі бар

АҚ режимін бұзатын салдарды талдау

АҚ бұзылу режимінің бағасы анықталады. АҚ режимінің бұзу салдары әртүрлі жоспарларда болуы мүмкін, мысалы тікелей қаржылық шығыны. Ақпараттық қауіпсіздік режимін бұзу салдары әртүрлі болуы мүмкін, мысалы: тікелей финанстық шығындар, беделдікті жоғалту, ресми құрылымдар жағынан жағымсыздық және т.б.

Берілген қадамда АҚ режимінің бұзылу салдарын бағалау үшін критерия жүйелері таңдалады және салдардың ауырлығын бағалау үшін интегралдау шкалалары қолданылады. Шкалалар мысалы 2.7-кестеде көрсетілген.

Тәуекелді бағалау

Берілген қадамда ақпараттық ресурстардың рұқсаттылығы, біртұтастығы және конфиденциялдық бұзылуының тәуелділік деңгейі өлшенеді. Тәуекелді деңгейі қауіп деңгейіне, осалдылық және салдардың бағаларына байланысты болады.

2.7-кесте

АҚ режиміндегі бұзылу салдарының ауырлығын бағалау

АҚ режиміндегі бұзылу салдарының ауырлық деңгейі	Анықтамалары
Жоғарғы	Уақиға бір немесе бірнеше көрінумен көрсетілген ұйым қызметкерлеріне күшті (апаттық) ықпалын тигізеді: - тікелей қаржылық шығынның үлкен жиынтығы (нақтылануы қажет); - қызметкерлердің денсаулығына тигізетін зардаптар (апат, мүгедектілік немесе қызметкердің ұзақ уақыт емделуі); - ұйым белсенділігінің төмендеуіне әкеп соқтыратын беделді жоғалту; - ұзақ уақыт ішіндегі ұйымшылдықты бұзу қызметі
Орташа	Бір немесе бірнеше жағдайларда болатын теріс шешімдерінің салдарына әкеп соқтырады: - тікелей қаржылық шығыннан көрінетін жиынтық (нақтылануы қажет); - іскерлік серіктестігінің жағымсыз реакциясы және тапсырыстар ағымдарын азайтуға шақыратын беделді жоғалту; - мемлекеттік органдар жағынан компанияның іскерлік белсенділігінің азаюы
Төменгі	Бір немесе бірнеше жағдайларда болатын теріс шешімдерінің салдарына әкеп соқтырады: - тікелей қаржылық шығынның шамалы жиынтығы (нақтылануы қажет); - қызметтегі кейбір жұмыстардың кедергілері тәртіп бұзушылық қызметтерінің уақытпен жалғастығы; - ақпараттық ресурстарды қалпына келтіру қажеттілігі

Тәуекелді өлшеудің бірнеше әдісі бар. Көбінесе 3-тарауда қарастырылған кестелік тәсілдер қолданылады.

Егерде сапалы тәсілдер қабылданса, АҚ тәуелділігін бұзу ықтималдылығы, шығынның ықпалдылық бағасы сияқты осалдылықпен қауіп деңгейі, сондай-ақ фактарлардың есебімен оның қауіп-қатер сатылары бойынша ранжирлануы керек.

Тәуекел сандық шкалалар көмегімен бағалануы мүмкін. Ол бақылау шаралары ұсынылған «құны - тиімділігі» критериясы бойынша серпімділік анализдерінің мүмкіндіктерін береді. Бірақ бұл жағдайдағы қабылдан-

ған модельді тепе-теңдікке тексеру және ішкі деректерді өлшеу шкалаларына қойылатын талаптар өте жоғары.

Тәуекелді басқару бойынша ұсыныстарды өңдеу

Тәуекелді азаюы бойынша деңгейге рұқсат еткенге дейін ұсыныстар қажетті болып табылады. Олар әртүрлі кешенді деңгейде мүмкіндігінше шараларды есептеу қажет, мысалы:

– АҚ саясатына өзгертулер енгізу;
– Нұсқаулардағы қызметтермен қызмет көрсетулердің уақытын өзгерту;
– Қосымша техника-бағдарламалық құралдар.

Құжаттардың қорытынды есеп беруін өңдеу

Құжаттардың есеп беру мазмұнына арнайы талаптар бар. Келесі бөлімдерді қарастырады:

– Жұмыс мақсаты;
– Қабылданған методология;
– АҚ бағытынан АЖ сипаттамасы;
– қауіптер;
– осалдылықтар;
– тәуекелділіктер;
– ұсынылатын бақылау шаралары.

2.5 АҚ бірлескен және тізілімделген стандарттарын басқару

Ұйымдардың және тізімдеменің жанында АҚ базалық деңгейі үшін өзінің спецификациясы көрсетілген. Төменде олардың кейбіреулері көрсетілген: XBSS базалық деңгей сервисінің спецификациясы, «Ақпараттық технологиялардың қауіпсіздігі» NASA стандарты және т.б.

2.5.1 X/Open қауіпсіздік сервисіндегі XBSS-спецификациясы

X/Open консорциум «АҚ базалық деңгей сервистерінің спецификациясы» деген атпен құжат шықты [6].

Спецификациялар типтік жобаларды шешу базасында құрылған ақпараттық жүйелерде қолданылады. Спецификацияны өңдегенде нақты критерия түрінде форматталған, «Good Practice» талаптарын қанағаттандыратын қорғаныс профилінің ұғымы пайдаланылады.

Спецификацияда төмендегілер анықталды:

– ақпараттық жүйелердің сервистеріне АҚ аймағындағы талаптар;
– АҚ талаптарына сәйкес келісім бойынша орнатылатын параметрлер.

Идентификация және аутентификация бағыныңқы жүйелеріне талаптар:

– айрықшыланбаған қолданушылар үшін әкімшілендіруге тыйым салынады;

– рұқсат топтары, орналасқан жері, уақыт бойынша шектеулік қою талап етіледі;

– парольді алмастыру алдында аутентификация қажет;

– жүйеге бірнеше сәтсіз кіру әрекетіндегі қауіпсіздік әкімшілігінің жедел тізбегі, келесі әрекеттің алдындағы қате енгізілген парольден кейінгі кедергі, жүйеге сәтсіз кіру әрекеттерін қадағалау орындалады;

– аутентификация және қолданушылар деректерін тіркеу үшін деректерді жүйелік қорғау;

– парольдерге (ұзындығы, жіберілетін символдары бойынша және т.б.) тексеру талап етіледі;

– экранға парольдің көрсетілуінде және жүйелік база пароліне рұқсатқа шектеу қойылған;

– аутентификацияда қажетті деректер қорғалады, ал парольдер тек шифрланған түрде сақталады;

– парольдерді ауыстырғанда, жаңа пароль ескі парольден ерекше болуы тиіс;

– қолданушылардың деректер базасы міндетті түрде аутентификациялланады;

– орнатқанда енгізілетін стандартты парольдердің алмастыруы жасалады; қолданушы жүйеге кіргенде соңғы кіріс/шығыстың, сервистердің, соңғы сәтсіз кіруінің уақыты туралы мәлімет береді.

Аудиттің/хаттаманың бағыныңқы жүйелеріне талаптар:

– хаттамаларға (тіркеуші журналы) жататын деректерді өзгертулерден қорғау қажет;

– жүйе ағымдағы оқиғаны көрсетуге және теңестіруге мүмкіндік беруі тиіс;

– қауіпсіздік әкімшілігінің құжаттамасын тізбектейтін тіркеу журналының біртұтастығын бұзуға әкелетін оқиғалар;

– деректер базасының рұқсатын хаттамалау міндетті болып табылады;

– деректер базасының объектілері, қолданушылары, қолданушы топтар үшін тіркеуге жататын оқиғаларды орнатады;

– басқару өкілеттілігімен қолданушылардың әрекеті ағымдағы жағдайдың тепе-теңдік аудитінің бұйымдарына ұшырайды;

– аудитті/хаттамалау құралы келесі кластардың оқиғасын қадағалап отыруға мүмкіндігі бар:

- идентификация және аутентификация механизмдерін қолдану;
- қолданушылардың мекен-жайлық кеңістігіне объектілерді орналастыру;

- объектіні құру, модификациялау, жою;
- қолданушы артықшылығының әрекеті;
- жұмыс шегіне деректердің берілісі;
- кіру нүкте сеанс жүйесінің жұмыс басталуы және аяқталуы;
- рұқсат және артықшылық құқықтарының модификациясы.

Хаттамалауға/аудитке минималды талаптар:

– жүйеге сәтті және сәтсіз кіру әрекетін тіркеу қажет;

– енгізетін деректер базасын басқару процесінде және жүйелік сервистерде өзгертулерді тіркеу қажет;

– тіркеу журналына рұқсат етілмеген рұқсат әрекетінде бұзушы процесін блоктап, қауіпсіздік әкімшілігіне хабарлама жіберу керек;

– тіркеу журналындағы оқиға туралы жазбаларды қолдану, сәтті/сәтсіз аяқталу, басталу күні, уақыты және оқиға (класта) типі туралы ақпараттан құрылуы қажет.

Рұқсатпен басқару жүйесіне қойылатын талаптар:

– рұқсатпен басқару үшін келесі атрибуттар қолданылады: қолданушы идентификаторы, оқуға, жазбаға, бағдарламаны орындауға, қолданушы профилі және бөлімше рұқсатының құқығы;

– рұқсат ережесінің атрибут рұқсатына негізделген және келісім бойынша рұқсат ережесінің орнатылуы;

– енгізу/шығару құрылымына рұқсат әкімшілігімен және техника-бағдарламалық шараларымен орындалады;

– деректер базасында субъект пен объект үшін атрибут рұқсаттары, сонымен объект атрибуты үшін импорт/экспорт операцияларының процесі орнатылады;

– рұқсат ережесі авторлықтан өткен қолданушыларға ғана таралады;

– рұқсатпен басқару ережесі бекітілген тізімдердің міндеттілері болып табылады;

– егер объектілер мен субъектілер үшін рұқсат ережесі бөлінсе, олардың келісімділігін тексеру қажет;

– қауіпсіздік саясатына жататын ақпаратты оқудан және модификациядан қорғауды, әсіресе аутентификация және идентификацияға байланысты деректерді, сонымен қатар жүйеге ену нүктелерін және оларға сәйкес параметрлерінің (қолданушылық және жүйелік) қауіпсіздігін қамтамасыз етуі қажет;

– қауіпсіздік саясатына қатысты және келісім бойынша орнатылған атрибуттарды жариялауға тыйым салынады;

– қолданушылар кез келген уақытта өзінің сеансын жабуға (тоқтатуға) және оны қайталанған аутентификациядан кейін қайта бастауға мүмкіндігі болуы қажет.

Объектілерді қайта пайдаланудан сақтау жүйесіне қойылатын талаптар:

– авторлық және атрибут қауіпсіздігіне байланысты барлық ақпараттар объектілерде болмайды, объектіні түсіргеннен кейін жадыдан (жою) алу керек;

– жүктемеген объектілерге жататын ақпаратты қолдануға рұқсатты (соның ішінде шифрленген) тыйым салу керек.

Критикалық ақпарат қорғанысының талаптары:

– қолданушының сеансы аяқталғаннан (блокталған) кейін қорытындыны тоқтату керек, ал мониторды жағу керек;

– Деректер базасының ағымдағы жағдайына байланысты ұйым туралы процедуралық сеанс инициализациясының қолданушыларға беру мүмкіндігі болу керек.

Біртұтастықты қамтамасыз ету құралдарына талаптар:

– процедураларды (шығаратын тапсырмалар) құжаттау қажет, соның ішінде деректердің бұзылуына және құрал-жабдықтардың жаңару жағдайында қайта қалпына келтіру сұрақтарын құжатталуы қажет;

– қолданушының жүйеге соңғы рет сәтті кіруі келесі ақпараттарға сүйенеді:

- кім соңғы рет жүйеге кірді (қолданушы, процесс және т.б.);
- кім соңғы рет жүйені енгізді (қолданушы, процесс және т.б.);
- жүйеге соңғы рет сәтті енгізу/шығарудың күні мен уақыты;
- сеанс уақытында пайдаланылған сервис;
- қолданушылық идентификатор туралы деректер;
- жүйеге сәтті кірудің/шығудың уақыты және күні;
- сеанс уақытындағы пайдаланылған сервис;
- соңғы сеанстың аяқталғанынан кейін жүйеге кірудің сәтсіз әрекет саны;
- қолданушы идентификаторы туралы деректер;

– деректер базасы жүйеге кірмеген қолданушылардың деректерге рұқсатын блоктау немесе тіркелмеген қолданушының жүйеге сәтсіз кіру әрекетіне шектеу қою қажет;

– деректер базасы үшін техникалық қызмет көрсету (технологиялық) режимінде және нормалық режимде жұмыс мүмкіндігін қамтамасыз ету;

– келісім бойынша қолданушылар үшін бағдарламалар және басқа қолданушылармен құрылған каталогтарға рұқсат жоқ;

– ақпараттық қауіпсіздікті қамтамасыз етумен байланысқан әкімшілер функциясы қолданушылармен процестерге қолы жетпейді;

– деректердің барлық категорияларын қалпына келтіру қорғаныстың минималды деңгейіне дейін деректердің жұмыс процедураларының шешімі міндетті болып табылады;

– қалпына келтіру процедурасын техникалық қызмет көрсету режимінде ғана жүргізуге болады.

Қол жетімділікті қамтамасыз ету құралдарына талаптар:

Берілген ақпараттық технологиялар үшін қол жетімділігіне талаптар қойылуы қажет.

Алынған және қайта шыққан ақпаратқа қауіпсіздікті қамтамасыз ету:

– қарапайым қолданушыларға жүйедегі қалыпты режимнен техникалық қызмет көрсету режиміне ауысуға мүмкіндік бермеу;

– қарапайым қолданушыларға техникалық қызмет көрсету режимінде жүйеге рұқсатын пайдалануға мүмкіндік бермеу;

– деректер базасы бөлек әрбір қолданушылар бойынша есеп беруді енгізу қажет.

АҚ басқару құралдарына талаптар:

– Қауіпсіздікті басқару құралдарының сенімдігі рөлдердің бөлуімен және әкімшелер міндеттерімен қамтамасыз етіледі;

– қолданушылар, жүйелік әкімшелер, қауіпсіздік әкімшелері қатысуы қажет;

– АҚ байланысқан қызмет міндеттерін қайта бөлу және толықтыру сұрақтарын ерекше бақылаған жөн;

– АҚ қатысты әкімшелендіру құралы оның рұқсат етілмеген орындалуын, модификациясын, жойылуын бақылайды;

– жаңа қолданушыларды тіркеу үшін жүйеге қорғаныс механизмі қажет;

– қорғаныс механизмінің қосып/өшіруінің мүмкін еместігін қамтамасыз ететін және оның деректер базасында болуы міндетті болып табылады; протоколдауға/аудитке жататын жағдайларды өзгерту немесе таңдау; қорғаныс атрибуттарының және жағдайдың келісімі бойынша орнатылғандарды өзгерту;

– ресми қолданушылардың сандары алынғаннан кейін, пассивті қолданушының уақытына шектеу талап етіледі;

– жүйелік әкімшілік бір немесе қолданушылардың таңдаған топтарына аудит амалын өткізу керек; ал аудитті өткізу құралы авторланбаған орындаудан, модификациядан, жоюдан қорғау қажет.

Деректер базасында:

- орнатқан механизмді таңдау және конфигурация параметрлерін жаңарту керек;
- әкімшіліктің кез келген орнатуы тек осыдан кейін ғана орындалуы мүмкін;
- қолданушылардың тіркеу параметрі рұқсат етілмеген жоюдан, модификациядан, танысудан қорғау механизмін қажет етеді;

• пассивті қолданушылардың жою механизмін қайта қарастыру қажет;

• әкімшілік қолданушылардың тізімнен жою командасын өзгертуге мүмкіндігі бар болу керек;

• әкімшілік функцияларының орындалуына тек автоматтандырылған қызметшілердің рұқсат беретін қорғаныс механизмі қажет.

2.5.2 NASA стандарты «Ақпараттық технологиялардың қауіпсіздігі»

Минимальды талаптар «Автоматтандырылған ақпараттық жүйелер үшін қауіпсіздік саясаты бойынша басшылық» құжаттарына сәйкес [7] және оның жағдайын нақтыландырады. Дифференциялдық тұрғыда, спецификацияланған талаптардың 30 позициясы бойынша 4 критикалық технология деңгейі енгізіледі. Мұндай тұрғылар (подход) оның спецификациясын қабылдауға мүмкіндік беретін және аталған әртүрлі технологиялардың типтері үшін базалық бірнеше нұсқаларының талаптық анықтамасы. Бұл құжат Internet-те ғана қол жетімді және оның спецификаларының есебімен ақпараттық қауіпсіздіктің бағыныңқы жүйесінде спецификацияны өңдеген өте пайдалы болып табылады.

ІІІ ТАРАУ

ТӘУЕКЕЛДЕРДІ ТАЛДАУ ТЕХНОЛОГИЯЛАРЫ

Ақпараттық тәуекелдерді талдау және оларды басқару сұрақтарына арналған әртүрлі ұйымдардың жарияланған құжаттары және ақпаратты қорғау саласындағы жоғарыда сипатталған стандарттардың практикада қолданылатын әдістемелерді жасауда міндетті түрде нақтыландыруды қажет ететін маңызды бөлшектердің қатарына ие емес. Бұл бөлшектерді нақтылаудың қажетті дәрежесі ұйымның даму деңгейінен, оның іс-әрекетінің спецификасынан және басқа факторлардың қатарынан тәуелді. Сонымен, тәуекелдерді басқарудың анықталған концепцияларына сәйкес келетін қандай да бір бірыңғай, отандық компаниялар мен ұйымдар үшін қолданысқа ыңғайлы әмбебап әдістемені ұсыну мүмкін емес. Әрбір жеке жағдайда тәуекелдерге талдау жасау және оларды басқарудың жалпы әдістемесін жеке өндірістің бизнесті жүргізуін және оның функциялау спецификасы мен нақты қажеттіліктерін есепке ала отырып бейімдеуге тура келеді.

3.1 Тәуекелдерге талдау жасау сұрақтары

3.1.1 Тәуекелдерді анықтау (идентификация – сәйкестендіру)

Кез келген әдістемеде тәуекелдерді анықтау керек, нұсқау ретінде олардың құрастырушылары алынады. Әрине, бұл жағдайда тізімнің толықтығы талап етіледі. Тізімді құрастыру есебінің қиындығы және оның толықтығының дәлелі тізімнің бөлшектелуіне қандай ұсыныстар талап етілендігінен тәуелді. Қауіпсіздіктің негізгі деңгейінде (ұйым дамуының үшінші деңгейі) кластардың бөлшектелуіне арнайы талаптар болмайды, сондықтан бұл жағдайда тәуекелдер класының қандай да бір ыңғайлы стандартты тізімімен қолданған жеткілікті. Негізгі деңгейдегі кейбір түр өзгешеліктер үшін қабылдауға болатын тәуекелдер шамасының бағасы қарастырылмайды. Тәуекелдер класының тізімдері басшылық қатарында, тәуекелдерге талдау жасауда арнайыланған БҚ-да (БҚ - бағдарламалық қамтамасыз ету) бар. Мысал – ақпараттық технологиялардың әртүрлі элементтеріне қолданылатын қауіптілік каталогы бар BSI Герман стандарты. Бұған сәйкес тізімдердің құндылығы олардың толықтығы болып табылады: ереже бойынша, мұндай кластар көп емес (ондықтар), олар жеткілікті кең және барлық табылатын тәуекелдердің жиынын жабады.

Мұндай есептеулерді тәуекелдердің кең емес (нақты) класына жүргізу ыңғайлы болғандықтан, кең кластарға контрөлшемдердің эффективтілігін және тәуекел деңгейін бағалау кемшілігі болып табылады. Мысалға алатын болсақ, «маршрутизатордың жөнделмегендігі» тәуекелдер класы ішкі кластардың жиынына бөлінуі мүмкін, олар БҚ жөнделмегендігімен бірге нақты маршрутизатор және жабдықтың жөнделмегендігінің мүмкін түрлерін алады.

3.1.2 Тәуекелдерді бағалау

Тәуекелдерді бағалауда келесі аспектілерді қарастыру ұсынылады:

– тәуекелдерді өлшеуге болатын шкалалар және критерийлер;

– оқиғалардың ықтималдықтарының бағасы;

– тәуекелдерді өлшеудің технологиялары.

Тәуекелдерді өлшеудің шкалалары мен критерийлері. Қандай да бір қасиетті өлшеу үшін шкаланы таңдау қажет. Шкалалар түзу (нақты) және жанама (өндіруші) болуы мүмкін. Физикалық шамаларды өлшеуге арналған шкалалар түзу шкалалардың мысалы болып табылады, мысалы сұйықтықтың көлемін литрмен өлшейтін шкалалар, ұзындықты метрмен өлшейтін шкалалар. Көп жағдайда түзу шкалалар табылмайды, бізді қызықтыратын сұрақтармен байланысты басқа қасиеттері бар түзу шкалаларды қолдануға тура келеді. Мысал – «ақпараттық қор құндылығының» субъективті қасиетін өлшейтін шкала. Бұл құндылық өндіруші шкалалардың өлшем бірлігінде өлшенуі мүмкін, олар қордың қайта қалпына келуінің бағасы, қордың қайта қалпына келуінің уақыты және т.с.с. Басқа нұсқасы, мысалы эксперттік бағаны алу үшін үш мәнге ие шкаланы анықтау:

– құндылығы аз ақпараттық қор: оған критикалық маңызды есептер тәуелді емес, сонымен қатар ол үлкен емес көлемдегі ақша және уақыт шығындарымен қайта қалпына келтірілуі мүмкін;

– құндылығы орташа қор: оған маңызды есептер қатары тәуелді, ал шығынға ұшыраған жағдайда ол критикалық мүмкіндіктерден аспайтын уақытта қайта қалпына келеді, бірақ қалпына келу құны жоғары болады;

– құнды қор (бағалы қор): оған критикалық маңызды есептер тәуелді, шығынға ұшыраған жағдайда қайта қалпына келу уақыты критикалық мүмкіндіктерден асып кетеді немесе қалпына келу бағасы шектен тыс жоғары.

Тәуекелдерді өлшейтін нақты шкалалар болмайды. Тәуекелдерді объективті немесе субъективті критерийлер бойынша бағалауға болады. Объективті критерийдің мысалы ретінде қандай да бір жабдықтың, мысалы ДК, белгілі уақыт интервалында қатардан шығып қалу ықтималдығын алуға болады. Субъективті критерийдің мысалы – ақпараттық қор иесінің ДК қатардан шығып қалу тәуекелінің бағасы. Әдетте, соңғы жағдайда бірнеше градациялы сапалы шкала жасалады, мысалы: төмен,

орташа, жоғары деңгей. Тәуекелдерге талдау жасау әдістемесінде сапалы бірліктермен өлшенетін субъективті критерийлер қолданылады, сондықтан:

– бағалау ақпараттық қорлар иесінің субъективті көзқарасын көрсетуі қажет;

– әртүрлі аспектілерді есепке алу керек, тек қана техникалық емес, сонымен қатар ұйымдық, психологиялық және т.с.с.

Қарастырылып отырған мысалда ДК-нің қатардан шығып қалу тәуекелінің бағасымен бірге субъективті бағаны алу үшін тікелей эксперттік бағаны қолдануға болады, не болмаса объективті түрде берілгендерді (ықтималдық) тәуекелдердің субъективті шкаласына түрлендіретін функцияны анықтауға болады.

Субъективті шкалалар сандық және сапалық болады, бірақ тәжірибеде 3-7 градациялы сапалық шкалалар қолданылады. Бір жағынан, бұл қарапайым және ыңғайлы, басқа жағынан, берілген мәліметтерді өңдеуге сауатты жолды қажет етеді.

Объективті және субъективті ықтималдықтар

«Ықтималдық» терминінің бірнеше әртүрлі мағыналары бар. «Объективті ықтималдық» және «субъективті ықтималдық» түсініктерінің қиылысуымен белгіленетін жиі кездесетін екі түсіндірмесі бар. Объективті ықтималдық деп (кейде физикалық деп аталатын) жалпы бақылаулар көлемінде қандай да бір оқиғаның пайда болуы жиілігінің қатынасы немесе қолайлы оқиғалар санының бақылаулардың жалпы санына қатынасы түсіндіріледі. Бұл түсінік бұрынғы уақытта орын алған саны үлкен бақылаулар нәтижесіне талдау жасауда, сонымен қатар қандай да бір процестерді сипаттайтын (пішіндердің) модельдердің салдары ретінде алынған нәтижелерде қолданылады.

Субъективті ықтималдық аясында қандай да бір адам немесе адамдар тобының берілген оқиға шынында да орын алатындығына сенімділік өлшемі түсіндіріледі. Субъективті ықтималдық деп берілген оқиға шынымен де орын алатындығына қандай да бір адамның немесе адамдар тобының сенімділігі. Оқиға пайда болу мүмкіндігінде субъективті ықтималдықтың әртүрлі тәсілдермен формалды ұсынылуы: оқиғалар жиынында ықтималдықтар үлестірімімен, оқиғалар жиынында бинарлық қатынаспен, толық емес берілген ықтималдықтар үлестірімімен немесе бинарлық қатынаспен немесе басқа да тәсілдермен. Субъективті ықтималдық көп жағдайда эксперттік жолмен алынған ықтималдылық өлшемді білдіреді. Дәл осы мағынада біз алдағы уақытта субъективті ықтималдықты түсінетін боламыз. Субъективті ықтималдық қазіргі кездегі жүйелік талдау жасау облысындағы жұмыстарда тек қана оқиғалар жиынында сенімділік өлшемін анықтауға мүмкіндік бермейді. Субъективті ықтималдық пен оның пайда-

лылығының арасындағы тығыз байланыс субъективті ықтималдықты алудың кейбір әдістерін құруда қолданылады.

Субъективті ықтималдықтың бағасын алу

Субъективті ықтималдықты алу процесін әдетте үш кезеңге бөледі: дайындық кезеңі, бағаларды алу, алынған бағаларға талдау жасау кезеңі.

Бірінші кезең. Бұл кезең уақытысында зерттеу объектісі – оқиғалар жиыны түзіледі, сонымен қатар осы жиын қасиеттерінің алғашқы талдауы жасалады (берілген оқиғалар жиынын туындататын оқиғалардың тәуелділігі немесе тәуелсіздігі, кездейсоқ шамалардың дискреттігі немесе үзіліссіздігі орнатылады). Осы талдаудың негізінде субъективті ықтималдықты анықтаудың ыңғайлы әдістерінің бірі таңдалады (негізгі әдістерге шолу 6-қосымшада қарастырылады). Осы кезеңде эксперт немесе эксперттер тобының дайындығы, олардың әдіспен танысуы және қойылған есепті түсінуінің тексерісі жүзеге асырылады.

Екінші кезең. Бұл кезең бірінші кезеңде таңдалған әдісті қолданудан тұрады. Бұл кезеңнің нәтижесі осы немесе басқа оқиға ықтималдығына эксперттің немесе эксперттер тобының субъективті көзқарасын бейнелейтін сандардың жиынтығы болып табылады, алайда жиі қарама-қайшылық болатындықтан барлық уақытта соңғы нақты үлестірілім болып саналмайды.

Үшінші кезең. Бұл кезеңде сұрақтардың нәтижелері зерттеледі. Егер эксперттер ұсынған ықтималдықтар ықтималдықтың аксиомаларымен келіспесе, онда бұған эксперттер назар аударады және жауаптар оларды таңдап алынған аксиомалар жүйесімен сәйкестендіру мақсатымен нақтыланады.

Субъективті ықтималдықты алудың кейбір әдістері үшін үшінші кезең болмайды, өйткені осы және басқа мағынада эксперттер бағалауына ең жақын болатындықтан әдістің өзі ықтималдықтар аксиомасына бағынатын ықтималдылық үлестірімін таңдаудан тұрады. Үшінші кезең эксперттер тобымен ұсынылған бағаларды агрегирлеу барысында ерекше маңызға ие болады.

3.1.3 Тәуекелдерді өлшеу

Қазіргі кезде тәуекелдерді өлшеудің бірнеше жолдары бар. Солардың ішінде мейлінше көп таралғаны, яғни тәуекелдерді екі және үш фактор бойынша бағалауды талқылаймыз.

Тәуекелдерді екі фактор бойынша бағалау

Қарапайым жағдайда екі фактор бойынша бағалау жасалады: оқиғаның ықтималдығы және мүмкін болатын салдарлардың ауырлығы. Әдетте тәуекел оқиғаның ықтималдығы және салдардың ауырлығынан үлкен

болады. Жалпы идея келесі формуламен өрнектеледі: ТӘУЕКЕЛ = $Р_{оқиға}$ × ЖОҒАЛТУ ҚҰНЫ.

Егер айнымалылар сандық шамалар болса, она тәуекел жоғалтудың математикалық күтімінің бағасы болып табылады.

Айнымалылар сапалық шамалар болған жағдайда көбейтудің метрикалық операциясы анықталмаған. Сонымен, бұл формуланы айқын түрде қолданып керек емес. Сапалық шамалардың қолданылу нұсқаларын қарастырамыз (ең жиі кездесетін жағдайларды).

Алдымен шкалалар анықталған болуы қажет:

Оқиға ықтималдығының сбуъектитві шкаласының мысалын келтіреміз:

A – тәжірибелік түрде оқиға ешқашан орындалмайды;

B – оқиға сирек болады;

C - қарастырылып отырған уақыт интервалында оқиға ықтималдығы - 0,5 шамасында;

D – ең болмағанда оқиға орындалады;

E – оқиға міндетті түрде орындалады.

Сонымен қатар, айталық, оқиға маңыздылығының субъективті шкаласы құрылады:

– N (Negligible)

– Mi (Minor)

– Mo (Moderate)

– S (Serious)

– C (Critical)

– N (Negligible) – ықпал еткенді елемеуге болады;

Mi (Minor) – болмашы оқиға: салдарлар жеңіл жойылады, салдарларды жою шығындары үлкен емес, ақпаратты технологияға ықпал ету болмашы;

Mo (Moderate) – нәтижелері бірыңғай оқиғалар: салдарларды жою үлкен шығындармен байланысты емес, ақпаратты технологияға ықпал ету үлкен емес және критикалық маңызды есептерге тимейді;

S (Serious) – салдарлары маңызды оқиға: салдарларды жою едәуір үлкен шығындармен байланысты, ақпаратты технологияға ықпал ету сезіледі, критикалық маңызды есептердің орындалуына әсер етеді;

C (Critical) – оқиға критикалық маңызды есептерді шешудің мүмкін еместігіне алып келеді.

Тәуекелдерді бағалау үшін үш мәннен тұратын шкала құрылады:

– төмен тәуекел;

– орташа тәуекел;

– жоғары тәуекел.

Нақты оқиғамен байланысты тәуекел екі факторға тәуелді және 3.1-кестедегідей анықталуы мүмкін.

3.1-кесте

Тәуекелді екі фактордан тәуелділік бойынша анықтау

Шкала	Negligible	Minor	Moderate	Serious	Critical
A	Төмен тәуекел	Төмен тәуекел	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел
B	Төмен тәуекел	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
C	Төмен тәуекел	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
D	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Орташа тәуекел	Жоғары тәуекел
E	Орташа тәуекел	Жоғары тәуекел	Жоғары тәуекел	Жоғары тәуекел	Жоғары тәуекел

Тәуекел факторларының шкаласы және кестенің өзі басқаша құрылуы мүмкін, басқа градация сандарына ие болу мүмкін.

Тәуекелдерді бағалаудың мұндай жолы жеткілікті түрде таралған.

Тәуекелдерді бағалаудың әдістемесін жасауда (қолдануда) келесі ерекшеліктерді есепке алған жөн:

– шкалалардың мәндері нақты анықталған болуы қажет (олардың сөздік сипаттамасы қажет) және экспертті бағалау процедурасының барлық қатысушыларымен бірдей түсіндірілуі керек;

– таңдалған кестенің негізделгендігі талап етіледі. Тәуекел факторларының бірдей үйлесуін сипаттайтын әртүрлі оқиғалар эксперттер көзқарасы тарапынан бірдей деңгейлі тәуекелге ие екендігіне көз жеткізуге болады.

Тәуекелдерді үш фактор бойынша бағалау

Базалық деңгейден жоғары талаптарға есептелген шетел әдістемелерінде тәуекелді үш фактор бойынша бағалау моделі қолданылады: қауіптілік, күдіктілік, жоғалтудың бағасы. Бұл әдістемелерде «қауіптілік» және «күдіктілік» сөздерінің аясында келесі түсінік беріледі.

Қауіптілік – ақпарат бүтіндігінің, қол жетімділігінің, конфиденциалдылығының бұзылу себебі болатын шарттар мен факторлардың жиынтығы.

Осалдық – қауіптіліктің жүзеге асуын мүмкін ететін ақпаратты қорғау жүйесіндегі әлсіздік.

Осы қолданыста объективті немесе субъективті шамалар болатын оқиға ықтималдығы қауіптілік және күдіктілік деңгейлерінен тәуелді:

$Р_{оқиға} = Р_{қауіптілік} \times Р_{осалдық}$

Сәйкесінше, тәуекел келесі түрде есептеледі:

ТӘУЕКЕЛ = $Р_{қауіптілік}$ х $Р_{осалдық}$ × ЖОҒАЛТУ БАҒАСЫ.

Егер сандық шкалалар қолданылатын болса, онда берілген өрнекті математикалық формула ретінде немесе, егер ең болмағанда бір шкала сапалық болатын болса, онда жалпы идеяның құрылымы ретінде қарастыруға болады. Соңғы жағдайда үш фактордан тәуелді тәуекелді есептеу үшін әртүрлі тектегі кестелік әдістер қолданылады.

Мысалы, 8 баллдық шкала бойынша тәуекел көрсеткіші келесі түрде өлшенеді:

1 – тәжірибе жүзінде тәуекел жоқ. Теория жүзінде оқиға орындалатын жағдайлар болуы мүмкін, бірақ тәжірибеде бұл сирек кездеседі, ал потенциалдық шығын салыстырмалы түрде көп емес;

2 – тәуекел өте аз. Бұған ұқсас оқиға сирек орын алады, сонымен қатар теріс салдарлар салыстырмалы түрде үлкен емес;

8 - тәуекел өте жоғары. Оқиға міндетті түрде орындалады және салдарлары өте ауыр.

Матрица 3.2-кестедегідей құрылуы мүмкін.

3.2-кесте.

Тәуекелді үш фактордан тәуелділік бойынша анықтау

Оқиға маңыздылығының дәрежесі (шығын бағасы)	Қауіптілік деңгейі								
	Осалдықтың төмен деңгейі			Осалдықтың орташа деңгейі			Осалдықтың жоғары деңгейі		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Берілген кестедегі Н, С, В күдіктілік деңгейлері сәйкесінше төмен, орташа, жоғары деңгейлерді білдіреді. Кестенің басқа да нұсқалары төменде 3.2.3 кестесінде қарастырылған.

Мұндай кестелер тәуекелдерді бағалаудың «қағаз» нұсқаларында, сонымен қатар БҚ секілді тәуекелдерге талдау жасаудағы әртүрлі тектегі құрал-жабдықтарда қолданылады.

Соңғы жағдайда матрица БҚ жасаушылармен беріледі, ол қайта жөндеуге жатпайды. Бұл осы тектес құралдардың дәлдігін шектейтін факторлардың бірі.

3.2 Қауіптілік және осалдылық бағаларының технологиясы

Қауіптілікті және осалдылықты бағалау үшін әртүрлі әдістер қолданылады, олардың негізінде келесілер жатуы мүмкін:

– эксперттік бағалар;

– статистикалық мәліметтер;

– қауіптілік және күдіктілік деңгейлеріне әсер ететін факторларды есепке алу.

Осындай әдістемелерді жасауда мүмкін жолдардың бірі – оқиға болғандығы жайлы статистикалық мәліметтердің жинақталуы, талдау жасау және олардың себептерінің классификациясы, олар тәуелді факторларды айқындау. Бұл ақпарат басқа да ақпараттық жүйелердегі қауіптіліктер және күдіктіліктерді бағалауға мүмкіндік береді.

Алайда тәжірибе жүзінде келесі қиындықтар орын алады.

Біріншіден, осы облыстағы оқиғалар жайлы жеткілікті ауқымды ақпарат жинақталуы қажет.

Екіншіден, бұл жол барлық уақытта ақталмайды. Егер ақпараттық жүйе ірі (құрамында көп элементі болса, сонымен бірге кең көлемде орналасқан болса), тарихы болса, онда бұл жол қолданысқа ыңғайлы. Егер де жүйе салыстырмалы түрде ірі емес және де технологияның жаңа элементтерін эксплуатация жасаса, онда қауіптілік және күдіктілік деңгейлері жалған болуы мүмкін.

Қазіргі уақытта кең таралған қауіптілік және күдіктілік деңгейлеріне әсер ететін әртүрлі факторды есепке ала отырып негізделген жол болып табылады. Ол маңызы аз техникалық детальдардан абстракциялануға, тек қана бағдарламалық техникалық емес, сонымен қатар басқа да аспектілерді назарға алуға мүмкіндік береді.

Тәуекелдер класының бірі үшін CRAMM 4.0 әдісінде қолданылатын сәйкес жолдың жүзеге асу мысалын қарастырамыз.

Ұйым қызметкерлерінің өзге идентификаторды пайдалануының тәуекелдер факторларының бағасы («маскарад»)

Қауіптілік бағасын беру үшін келесі жанама факторлар таңдалған:

– тіркелген оқиғалар (инцидент - оқиға) бойынша статистика;

– сәйкес бұзылымдар бойынша статистикадағы тенденциялар (ой мақсат);

– потенциалды ішкі және сыртқы бұзылымдар үшін қызығушылық келтіретін ақпараттық жүйелердің бар болуы;

– қызметкерлер құрамының моральдық сапасы;

– ақпараттық жүйедегі өңдеуден өзгертілген пайданы шығару мүмкіндігі;

– ақпаратқа кірудің балама (альтернативті) тәсілдерінің бар болуы;

– ұйымның басқа ақпараттық жүйелердегі сәйкес бұзылымдар бойынша статистикасы.

Осалдылық бағасы келесі жанама факторлардың негізінде орындалады:

– жүйедегі жұмысшы орындарының (пайдаланушы) саны;

– жұмысшы топтарының мөлшері (көлемі);

– қызметкерлердің іс-әрекеттері жайында басшылықтың хабардар болуы (әртүрлі аспекті);

– жұмыс орындарында құрылған жабдықтардың және БҚ-ның мінездемесі;

– пайдаланушылардың өкілеттілігі.

Жанама факторлар бойынша белгілі бір балл «тұратын» сұрақтар және кейбір бекітілген жауаптардың нұсқалары ұсынылады. Берілген кластың қауіптілік және күдіктіліктің қорытынды бағасы балдарды қосындылау жолымен анықталады.

Қауіптілік бағасы

Сұрақтарға жауап беріңіз.

1. Соңғы үш жылда ұйымның қызметкерлері қанша рет басқа пайдаланушылардың құқығын қолданумен ақпараттық жүйедегі сақталған ақпаратқа санкцияланбаған мүмкіндік алуға ұмтылды?

Жауаптардың нұсқалары

a	Бір ретте емес	0
b	Бір немесе екі рет	10
c	Жылына орташа бір рет	20
d	Жылына орташа бір реттен жиі	30
e	Белгісіз	10

2. Ақпараттық жүйеге осындай тектегі санкцияланбаған ұмтылыстардың статистикадағы тенденциясы қандай?

Жауаптардың нұсқалары

a	Өсуге қарай	10
b	Тұрақты болып қалу	0
c	Кемуге қарай	-10

3. Ақпараттық жүйеде ұйым қызметкерлерінің қызығушылығын тудыратын және оған санкцияланбаған мүмкіндік алуға итермелейтін ақпарат сақтала ма?

Жауаптардың нұсқалары

a	Иә	5
b	Жоқ	0

4. Қызметкерлерге өзге адамдар тарапынан көрсетілген қауіп-қатер, қорқыту, қысым көрсету жағдайлары белгілі ме?

Жауаптардың нұсқалары

A	Иә	5
B	Жоқ	0

5. Топ ішінде немесе жекелеген адамдар арасында жоғары моральдық сапалары жеткілікті емес адамдар бар ма?

Жауаптардың нұсқалары

a	Жоқ, барлық қызметкерлер жоғары адалдықпен және ұқыптылықпен ерекшеленеді.	0
b	Жоғары моральдық сапалары жеткілікті емес адамдар тобы немесе жеке тұлғалар бар, бірақ бұл оларды жүйені санкцияланбаған пайдалануға	5
c	Моральдық сапалары соншалықты төмен адамдар тобы немесе жеке тұлғалар бар, бұл қызметкерлердің жүйені санкцияланбаған түрде пайдалану ықтималдығын жоғарылатады.	10

6. Жүйеде санкцияланбаған өзгеріс қызметкерге тікелей пайда әкелетін ақпарат сақтала ма?

Жауаптардың нұсқалары

a	Иә	5
b	Жоқ	0

7. Сәйкес іс-әрекеттерді техникалық мүмкіндіктерге ие пайдаланушыларды қолдау ақпараттық жүйеде қарастырылған ба?

Жауаптардың нұсқалары

a	Иә	0
b	Жоқ	5

8. «Маскарадты» қолданғаннан гөрі, ниеті жаман адамға ақпаратты көруге мүмкіндік беретін одан қарапайым басқа тәсілдері бар ма?

Жауаптардың нұсқалары

a	Иә	-10
b	Жоқ	0

9. «Маскарадты» қолданғаннан гөрі, ниеті жаман адамға қалаған нәтижесіне жету үшін ақпаратты санкцияланбаған түрде өзгертуге беретін одан қарапайым басқа тәсілдері бар ма?

Жауаптардың нұсқалары

a	Иә	-10
b	Жоқ	0

10. Соңғы үш жылда қызметкерлер сіздің ұйымыңыздағы басқа ұқсас жүйелерде сақтаулы тұрған ақпаратқа санкцияланбаған мүмкіндік алуға қанша рет ұмтылды?

Жауаптардың нұсқалары

a	Бір ретте емес	0
Ь	Бір немесе екі рет	5
c	Жылына орташа бір рет	10
d	Жылына орташа бір реттен жиі	15
e	Белгісіз	10

Балдарды қосқандағы қауіптілік дәрежесі

9-ға дейін	Өте төмен
10-нан 19-ға дейін	Төмен
20-нан 29-ға дейін	Орташа
30-нан 39-ға дейін	Жоғары
40 және одан да жоғары	Өте жоғары

*Осалдылық **бағасы***

Сұрақтарға жауаптар.

1. Ақпараттық жүйемен пайдалануға қанша адамның құқығы бар?

Жауаптардың нұсқалары

a	1-ден 10-ға дейін	0
b	11-ден 50-ге дейін	4
c	51-ден 200-ге дейін	10
d	200-ден 1000-ға дейін	14
e	1000-нан жоғары	20

2. Ұйым басшылығы оның басында жұмыс жасап жүрген қызметкерлер өздерін басқаша ұстап жүргендерінен хабардар бола ма?

Жауаптардың нұсқалары

a	Иә	0
b	Жоқ	10

3. Пайдаланушыларға қандай қондырғылар және бағдарламалар қол жетерліктей мүмкіндікте?

Жауаптардың нұсқалары

a	Ақпараттың маршрутизациясына және жеткізілуіне, бірақ берілгендердің жетуіне емес, жауапты тек қана терминалдар немесе желілік бақылаушылар	-5
b	Тек қана стандартты офистік қондырғылар және бағдарламалар, сонымен қатар мәзір көмегімен басқарылатын бағынышты қолданбалы бағдарламалар	0
c	Пайдаланушылар операциялық жүйеге кіруге мүмкіндік алуы мүмкін, бірақ компиляторларға емес	5
d	Пайдаланушылар компиляторларға мүмкіндік алады	10

4. Қызметкерлерге алдын ала ескертілген жұмыстан шығу немесе қысқарту жайында ескертілген жағдайда, ақпараттық жүйеге логикалық мүмкіндікке рұқсат беріле ме?

Жауаптардың нұсқалары

a	Иә	10
b	Жоқ	0

5. Ақпараттық жүйеге мүмкіндігі бар пайдаланушы бөлімшелер қызметкерлерінің жұмысшы топтарының орташа мөлшері қандай?

Жауаптардың нұсқалары

a	10-нан аз адам	0
b	Адам саны 11-ден 20-ға дейін	5
c	20 адамнан жоғары	10

6. Ақпараттық жүйедегі сақтаулы тұрған мәліметтерді бірден бірнеше адамға айқын етіп өзгерту факт болып есептеле ме?

Жауаптардың нұсқалары

a	Иә	0
b	Жоқ	10

7. Пайдаланушыларға мәліметтер жүйесіндегі барлық сақталғандарға ресми түрде мүмкіндік беру қаншалықты үлкен?

Жауаптардың нұсқалары

a	Ресми құқық барлық пайдаланушыларға берілген	-2
b	Ресми құқық тек қана кейбір пайдаланушыларға берілген	0

8. Жүйедегі сақтаулы тұрған барлық ақпаратты білу пайдаланушыға қаншалықты қажет?

Жауаптардың нұсқалары

a	Барлық ақпаратты барлық пайдаланушыға білу қажет	-4
b	Жекелеген пайдаланушыларға тек қана оған қатысты ақпаратты білу ғана қажет	0

Балдарды қосқандағы осалдылық дәрежесі

9-ға дейін	Төмен
10-нан 19-ға дейін	Орташа
20 және одан да жоғары	Жоғары

3.3 Тәуекелдерге басқарудың сұрақтары

Берілген қолдың күмәнсіз артықшылығы көптеген жанама факторларды есепке алу мүмкіндігі болып табылады (тек қана техникалық емес). Әдістеме қарапайым және ақпараттық қорлар иесіне қандай жолмен қорытынды баға алынатынына және бағаларды жақсарту үшін не істеу керек екендігіне айқын ұсыныс береді.

Кемшіліктеріне жанама факторлар және олардың салмақтары ұйымның іс-әрекет сферасынан тәуелді, сонымен қатар басқа да жағдайлардың қатары жатады. Сонымен, әдістеменің әрқашан нақты объект бойынша ыңғайланып құрылуын талап етеді. Сонымен қатар таңдап алынған жанама факторлардың толықтығы және олардың салмақ коэффициенттерінің дұрыстығы – формалдылығы аз және қиын есеп, ол практикада эксперттік әдістермен шешіледі (әдістеме бойынша алынған нәтижелердің күтілген тесттік жағдайлармен сәйкестігі тексеріледі).

Ұқсас әдістемелер анықталған профильді ұйымдар үшін жасалады, апробацияланады және соңынан ведомсттік стандарт ретінде қолданылады. Осы жолмен CRAMM бағдарламасын құрушылар да жүрді, олар әртүрлі ведомстволар үшін ондаған нұсқалар шығарды (сыртқы істер министрлігі, қарулы күштер және т.с.с.).

Қарастырылған мысалдағы тәуекелдер және күдіктіліктер бағалары сапалық шамалар болып табылады. Алайда ұқсас әдістермен қалдық тәуекелдерді есептеуде және басқару есептерін шешуде қажет болып табылатын сандық бағалар да алынуы мүмкін. Бұл үшін арақашықтықтар жүйесін бағалайтын реттелген жиынды құруға мүмкіндік беретін (жалпы шолу 6-қосымшада келтіріледі) бірнеше әдістер қатары қолданылады.

Тәуекелдердің объективті сандық бағаларын алу ақпараттық тәуекелдерді сақтандырумен айналысатын сақтандыру агентстволары үшін өзекті болуы қажет.

Тәжірибеде көп жағдайда сақтандыру агенттіктері сапалық бағалармен айналысады. Қарапайым әдістемелер ұзақ емес және қымбатқа түспейтін зерттеулер ақпараттық жүйені қызметкерлер қатарымен сұхбат негізінде осы немесе басқа тәуекелдер тобына (сақтандыру компаниясының классификациясы бойынша) жатқызуға мүмкіндік береді. Мұндай әдістемелерде сонымен қатар жанама факторлар бекітіліп, оларға талдау жасалады.

Мүмкін болатын тәуекел деңгейін таңдау ақпараттық қауіпсіздіктің ішкі жүйелерін жүзеге асыруға кететін шығындармен байланысты. Мүмкін болатын тәуекел деңгейін таңдаудың кем дегенде екі жолы бар.

Бірінші жол қауіпсіздіктің базалық деңгейі үшін типтік болып табылады. Қалдық тәуекелдер деңгейі назарға алынбайды. Ақпараттық жүйенің базалық деңгейіндегі спецификасына (антивирустық БҚ, МЭ, резервтік көшіру жүйесі, қол жетімділікті бақылау жүйесі) сәйкес келетін бағ-

дарламалық-техникалық қорғау жабдықтарына кететін шығындар және ұйымдық іс-шаралар міндетті болып табылады, олардың мақсаттылығы талқыланбайды. Қосымша шығындар (егер мұндай сұрақ ИБ аудиті жүргізген нәтижелер бойынша немесе қауіпсіздік қызметінің инициативасы қойылған болса) шектен шықпауы керек және ақпараттық жүйенің қолдауына кететін шығынның 5-15%-дан аспауы қажет.

Екінші жол қауіпсіздіктің жоғары деңгейін қамтамасыз ету үшін қолданылады. Ақпараттық қор иесі қалдық тәуекелдердің мүмкін болатын деңгейін өзі таңдауы және өзінің таңдауына жауап беруі қажет.

Ұйым дамуының деңгейінен және негізгі іс-әрекеттің сипаттамасынан мүмкін болатын тәуекел деңгейін таңдауды негіздеу әртүрлі әдіспен жүргізіледі.

Қорғаудың әртүрлі нұсқаларының ең кең таралғаны «құндылық-эффективтілік» критерийі бойынша талдау жасау болып табылады. Есептің қойылымының мысалдарын келтіреміз:

1) ішкі жүйе қауіпсіздігінің құны ақпараттық жүйе құнының 20%-нан аспауы қажет. Интегралдық тәуекелдер деңгейін максималды азайтатын контрөлшем нұсқасын табу керек;

2) барлық кластар бойынша тәуекелдер өте төмен деңгейден аспауы керек. Құны минимал болатын контрөлшемдер табу керек.

Егер басқару есебі қойылатын болса, онда контрөлшемдер кешенін дұрыс таңдау (мүмкін болатын нұсқаларды есепке алу) және оның эффективтілігін бағалау маңызды.

3.4 Тәуекелдерді талдаудың корпоративтік әдістемесін жасау

Ақпараттық тәуекелдерге талдау жасау өндірістің ақпараттық қауіпсіздігін эффективті басқаруға мүмкіндік береді. Бұл үшін тәуекелдерге талдау жасау жұмысының басында өндірісте нақты нені қорғау керек және ол қандай қауіпке ұшырауы мүмкін екендігін анықтап алу қажет, ал одан кейін қорғау тәжірибесі бойынша ұсыныстарды қолдану кажет. Енді компанияның ақпараттық тәуекелдерін басқару және оларға талдау жасаудың өзіміздің жеке әдістемемізді қалай жасау керектігін талқылаймыз.

Мұндай талдау конфиденциалды мінездемеге ие ақпараттың нақты түрін қорғаудың есебі мен непосредственный мақсаттардан бастау алады. Мұндай ақпаратты қорғаудың аясындағы маңызды есептердің бірі – бүтіндігі мен қол жетімділігін қамтамасыз ету. Көп жағдайда бүтіндіктің бұзылуы алдын ала жасалған іс-әрекеттің салдары ретінде ғана емес, басқа да себептердің қатарынан болуы мүмкін: ақпаратты жоғалтудың немесе тарылуына әкеп соқтыратын жабдықтардың бұзылуы. Сондықтан «шабуыл» терминінің аясында ақпараттық қорларға тек қана адамдық емес, сонымен бірге өндірістің ақпаратын өңдейтін жүйе қоршаған ортаның әсерлерін түсінеміз.

Тәуекелді талдаудың алты кезеңінің әрбірі нақтыланған болуы қажет.

Бірінші және екінші кезеңдерде өндіріс үшін коммерциялық құпия болып табылатын, қорғауға тиіс мәліметтер айтылады. Мұндай мәліметтердің арнайы орындарда және нақты жабдықтарда сақталатыны түсінікті, олар байланыс каналы бойынша беріледі және қабылданған регламентке сәйкес өңделеді. Сонымен қатар ақпаратпен айналысудың технологиясындағы негізгі фактор КАЖ архитектурасы болып табылады, одан көп жағдайда өндірістің ақпараттық қорларының қауіпсіздігі тәуелді болады. Осымен байланысты қайталап айтатын нәрсе ақпараттық қауіпсіздіктің дәрежесі тек қана қорғаудың әдіс және тәсілдерімен ғана емес (соншалықты болмауы да мүмкін), сонымен бірге КАЖ құрылуының ерекшеліктерімен де анықталады. Орындалған қорғануда КАЖ жайында айтқанда, ең алдымен ақпаратты өңдеудің осындай архитектурасын (топологиясын) таңдауы жайында, ақпаратқа қол жетімділік мүмкіндігінің ықтимал сандарын азайтатын конфиденциалды ақпаратты өңдейтін құралдардың орны және оның сақталуы, жіберілуі сөз болады.

Тәуекелді талдаудың үшінші кезеңі – мүмкіндік каналдарының схемасын құру. Әрбір мүмкіндік каналы нүктелер жиынымен сипатталады, олардан ақпаратты «алуға» болады. Олар күдіктілікті білдіреді және ақпаратқа жағымсыз іс-әрекеттерді қолданбауды талап етеді.

Шабуылдың барлық мүмкін нүктелерін қорғаудың талдауы қорғау мақсаттарына сәйкес келеді, бұл төртінші кезең.

Бесінші кезеңде осы уақытқа дейінгі белгілі әдістерден әрбір мүмкін болған шабуыл нүктесі бойынша қауіптіліктің жүзеге асу ықтималдығы табылады.

Қорытынды кезеңде әрбір шабуылдың жүзеге асу жағдайындағы ұйымға келетін шығынның бағасы жасалады. Бұл мәліметтер күдіктілік бағаларымен бірге ақпараттық қорға келетін рангылау тізімін алуға мүмкіндік береді.

Жұмыстың нәтижесі ақпаратты қорғау жүйесін өзгерту шешімін жасау және қабылдау қабылдауға ыңғайлы түрде ұсыну болып табылады. Бұл жағдайда әрбір ақпараттық қор бірнеше потенциалды қауіптіліктерге ұшырау мүмкіндігі маңызды. Ақпараттық жүйеге қол жетімділіктің қосынды ықтималдығы принципиальді мағынаға ие болады, ол ақпараттың жеке нүктелерге жету ықтималдықтарының қосындысы.

Әрбір қор бойынша ақпараттық тәуекел шамасы – бұл ақпаратқа шабуыл және қауіптіліктің жүзеге асу ықтималдықтарының көбейтіндісі. Бұл көбейтіндіде құрамындағыларды өлшеудің әртүрлі әдістері кездеседі.

Тәуекелдерді барлық қорлар бойынша біріктіру КАЖ архитектурасы бойынша қабылданған және оған ақпаратты қорғау жүйесін енгізудегі тәуекелдердің жалпы шамасын береді.

Сонымен, ақпаратты қорғау жүйесін және КАЖ архитектурасын вариациялау арқылы (қауіптіліктің жүзеге асу ықтималдығы өзгеруі есебінен) тәуекелдердің әртүрлі мәндерін қарастыруға болады. Бұл жерде ең маңызды қадам шешім қабылдаудың берілген критерийлерімен сәйкес келетін бір нұсқаны таңдау болып табылады. Ондай критерий тәуекелдің мүмкін болатын шамасы немесе ақпараттық қауіпсіздікпен қамтамасыз ету шығынының қалдық тәуекелге қатынасы болуы мүмкін.

Ақпараттық қауіпсіздікпен қамтамасыз ету жүйесін құруда өндірісте тәуекелдерді басқару стратегиясын анықтау қажет.

Қазіргі кезде тәуекелдерді басқарудың бірнеше жолдары белгілі. Олардың ішінде ең кең таралғаны – бағдарламалық-техникалық және ұйымның қорғау өлшемдерін қамтитын кешенді контрөлшемдер жүйесін қабылдау арқылы тәуекелді азайту болып табылады. Тәуекелден ауытқумен байланысты жол жақын болып табылады. Кейбір тәуекелдер класынан ауытқуға болады, мысалы: ұйымның Web-серверінің локальді желі шегінен шығарылуы Web-клиенттер жағынан локальді желіге санкцияланбаған қол жетімділікке ие болу тәуекелінен сақтануға мүмкіндік береді.

Ең соңында көп жағдайлар қатарында тәуекелді қабылдау мүмкін жағдай. Бұл жағдайда келесі дилемманы анықтау маңызды: өндіріс үшін не маңызды – тәуекелдермен күресу ме әлде оның салдарларымен бе? Бұл жерде тиімділік есебін шешуге тура келеді.

Тәуекелдерді басқару стратегиясы таңдалғаннан кейін ақпараттық қордың қорғалғандығы туралы эксперттік қорытындының дайындығымен бірге ақпараттық қауіпсіздікпен қамтамасыз ету бойынша іс-шаралардың қорытынды бағасы жүргізіледі. Эксперттік қорытындыға тәуекелдерге талдау жасау және оларды төмендетуге байланысты барлық материалдар кіреді.

Тәуекелдерге жасалатын талдаудың орындалуы және шығындардың бағасы ақпаратты қорғау мәселелерімен байланысты көптеген салаларда терең жүйелік білімдерді және аналитикалық ойлауды талап етеді.

3.5 Тәуекелдерге талдау жасаудың Microsoft әдістемесі

Тәуекелдерге талдау жасаудың корпоративтік әдістемесінің мүмкін мысалы ретінде Microsoft компаниясының әдістемесін қарастырамыз.

Әдістемеде тәуекел желінің ішкі немесе сыртқы қауіпсіздігінің бұзылуына байланысты шығын әкелуші мүмкіндік ретінде анықталады. Ақпараттық қауіпсіздік сферасындағы өндірістің тәуекелдерді басқаруы келесі төрт кезеңнің орындалуын талап етеді:

1) тәуекелдерді тану (идентификация);
2) тәуекелдің өлшемін анықтау;
3) тәуекелдерді басқарудың жоспарын құру;
4) тәуекелдерді басқару және ағымдағы бақылау;

Тәуекелдерді танудағы шектеулі уақытта эксперттерден мәліметтер алу әдістемесін қолдану ұсынылады, жекелей алғанда «ми штурмы» әдісі. Тәуекелдің әрбір пайда болуына оны бағалау (егер қарастырылып отырған ұнамсыз оқиға болған жағдайда шығынды анықтау) және тәуекелдің пайда болу ықтималдығын анықтау талап етіледі.

Әрбір қауіптілікті бағалау келесі әдістермен жүзеге асуы мүмкін:

– шабуылдау тобын пайдаланумен бірге мамандар тобы жүйесінің шабуылына ұқсатылады;

– идеяларды жинау әдісімен мүмкін болатын тәуекелдерді талқылайтын және контрөлшемдерді ұсынатын қызметкерлер немесе кеңес берушілер тобы құрылады;

– қауіптіліктің формалды бағаларын қолдану жолымен, тәуекелдерді басқару әдістері және қорғаныштық өлшемдерінің интеграциясы.

Тәуекелдерді бағалаудың ұсынылып отырған Microsoft стратегиясы келесі кезеңдерден тұрады:

– тәуекелдің мүмкін болатын деңгейін анықтау (яғни тәуекелдің қабылданылатын деңгейін);

– әрбір тәуекелдің пайда болу ықтималдығының бағасы;

– әрбір тәуекелге құн беру;

– приоритеттерді орналастырып қою.

Әрбір тәуекелге баға беру процесінде оның пайда болу ықтималдығы және онымен бірге болатын шығындар мөлшері есептеледі. Алдағы уақытта тәуекелдерді бағалаудың кестелік түрі қолданылады, келесі түрдегі матрица құрылады:

3.7-кесте

Факторлардан тәуелді тәуекелдің кестелік бағасы

Ықтималдық	Құны		
	Жоғары	Орташа	Төмен
Жоғары	Қызыл	Қызыл	Көк
Орташа	Сары	Сары	Жасыл
Төмен	Көк	Көк	Жасыл

Алынған бағадан тәуелділігіне байланысты тәуекел келесі топтардың біріне жатады:

– жоғары тәуекел (қызыл облыс). Мұндай тәуекелдерді төмендетпей өндірістің ақпараттық жүйелерге қарауы бизнеске кері әсерін тигізуі мүмкін;

– табылатын тәуекел (сары облыс). Бұл жағдайда теріс салдарларын азайтуға немесе толығымен жоюға мүмкіндік беретін тәуекелдерді басқарудың эффективті стратегиясы талап етіледі;

– тәуекел (көк облыс). Бұл облысқа түскен тәуекелдер қатынасына оларды басқарудың негізгі процедураларын қолдану жеткілікті;

– ықпал етпейтін тәуекел (жасыл облыс). Бұл жағдайда тәуекелдерді басқаруға күш салу аса маңызды рөл ойнамайды.

Мүмкін болатын деңгей негізінде (мүмкін болатын тәуекелдер деңгейі) потенциалдық шығындар мөлшері және тәуекелдердің пайда болу ықтималдықтарына приоритеттер бекітіледі. Олар ең алдымен шабуыл жасайтын тәуекелдерді анықтауға көмектеседі және ол тәуекелдерді басқарудың жоспары құрылады.

Жоспарлау келесімен қорытындыланады:

– әрбір тәуекел үшін триггерлерді анықтау;

– Іс-шаралардың жоспарларын, күтпеген оқиғаларға әсер ету жоспарларын және әрбір тәуекелдің зардаптарын азайту жоспарын дайындау.

Тәуекелдерді басқаруды жоспарлаудың төрт бөлімі ерекшеленеді:

– зерттеу;

– қабылдау (берілген тәуекелді қабылдауға бола ма?);

– басқару (тәуекелді азайту үшін шара қолдануға бола ма?);

– шығару (тәуекелді жою немесе блоктау үшін не істеуге болады?).

Бұл жағдайда зерттеу әрбір тәуекелге қатысты қолданылады, ал қалған стадиялар комбинациялануы мүмкін. Айталық, жүйені зерттеу көрсеткендей өндірісте потенциалды күдікті қосымша орнатылған, бұл сәтте онымен жұмыс істеуге толық қарсы болу мүмкін емес. Айталық, алдағы уақытта берілген қосымша мүмкін болатын барлық түйіндерде өшірілген, ал қалғандарында сәйкесінше қалған. Бұдан шығатыны, бұл тәуекелдің қатынасына қарай келесі кезеңдер орындалған: зерттеу, жою (бөліктеп), қабылдау (бөліктеп).

Ішкі және сыртқы шарттарды өзгерткенде алдыңғы уақытта жасалған тәуекелдер бағалауына коррекция жасау болып табылатын тәуекелдерді бақылау есебі де маңызды.

IV ТАРАУ

ТӘУЕКЕЛДЕРДІ ТАЛДАУДЫҢ ПРОГРАММАЛЫҚ ҚҰРАЛДАРЫ

Тәуекелдерді талдаудың программалық құралдары ақпараттарды қорғау облысындағы кәсіпорынның ақпараттық тәуекелдерін бағалайтын немесе қайта бағалайтын мамандардың жұмысын автоматтандыруға мүмкіндік береді.

Қазіргі таңда Қазақстанда «қағаз» әдістемесінің көптеген түрлері жиі қолданысқа ие. Әдетте мұндай әдістерді жасап шығарумен ақпараттарды қорғау облысындағы жүйелік және мамандандырылған интеграторлар болып табылатын компаниялар айналысады. Белгілі бір себептерге байланысты әдістемелер әдетте жарияланбайды, өйткені олар компанияның «know how»-на жатады. Осындай әдістемелерге қол жеткізу қиын болғандықтан, олардың сапасы, обьективтілігі және де мүмкіншіліктері туралы шешім шығару күрделі болып табылады.

Тәуекелдерді талдау әдістемесіне негізделген арнайы программалық өнімдердің категориясына жата алады немесе кәсіпорынның жеке меншігінде болады, яғни сатылмайды. Егер программалық жабдық өнім ретінде шығарылса, онда ол белгілі бір дәрежеде әмбебап болуы қажет. Программалық жабдық ведомствалық нұсқалары тәуекелдерді талдау және басқару есептерінің қойылу ерекшеліктеріне бейімделіп және кәсіпорынның ақпараттық жүйелерінің ерекшелігін ескеруге мүмкіндік береді.

Нарықтағы ұсынылып отырған программалық жабдық негізінде қауіпсіздіктің базалық деңгейінен асатын ақпараттық қауіпсіздіктің деңгейіне негізделген. Сондықтан құрал-сайман, бірінші тарауда айтылған, даму деңгейі 3-4 дәрежелік кәсіпорындар қажеттіліктеріне негізделген.

2000 жылы BS 7799 британдық стандарты негізінде жасалған ISO 27001 халықаралық стандарты қабылданды. Нәтижесінде көптеген программалық құралдар (тәуекелдерді талдаудың программалық жабдықтары) дәл осы стандарттың талаптарына сай болатындай етіп түрлендірілді. Арнайы программалық жабдық шартты түрде екі топқа бөлінеді: базалық деңгейдегі программалық жабдық және тәуекелдерді талдаудың толық программалық жабдық.

Тәуекелдерді толық талдаудың программалық әдістері жүйелік талдау және жобалау құрылымдық әдістерін қолданып құрылады (SSADM - Structured Systems Analysis and Design) және құрудың автоматизация-

ланған әдістер категорияларына немесе CASE-әдістеріне (Computer Aided System Engineering) жатады.

Осындай әдістер келесілер үшін құрал-сайман болып табылады:

– АҚ позициясымен АЖ моделін құру;

– қорлардың құндылықтарын бағалау;

– қауіп-қатерлердің тізімін құру және олардың ықтималдықтарын бағалау;

– контршараларды таңдау және олардың тиімділігін талдау;

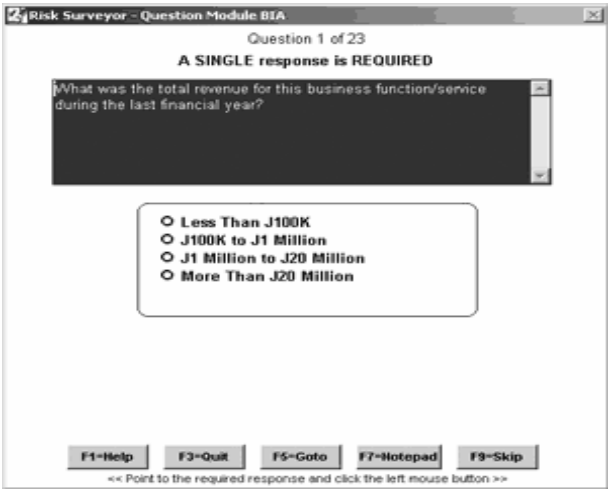
– қорғанысты құрудың нұсқаларын талдау;

– құжаттау (есеп берулерді генерациялау).

COBRA

Тәуекелдерді талдауға және басқаруға арналған программалық өнім – COBRA, өндіруші - C&A Systems Security Ltd., ол ақпараттық қауіпсіздік режимінің BS 7799 (ISO 27001) британдық стандартының талаптарына сай келетінін тексеретін процесті түрлендіруге және тездетуге мүмкіндік береді, сонымен қатар тәуекелдерді талдаудың қарапайым түрін жүргізеді. Бірнеше мәліметтер қоры бар: BS 7799 (ISO 27001) жалпы талаптары және кез келген қолдану аймағына негізделген арнайы қорлар. Бұл программалық жабдық көркемделген нұсқасы бар.

COBRA стандарттың талаптарын тематикалық «сұраулар» түрінде кәсіпорынның жеке қызмет аспектілері бойынша көрсетуге мүмкіндік береді (4.1-суретте мысал келтірілген).



4.1-сурет. Cobra программалық жабдық қолданып тәуекелдерді талдау

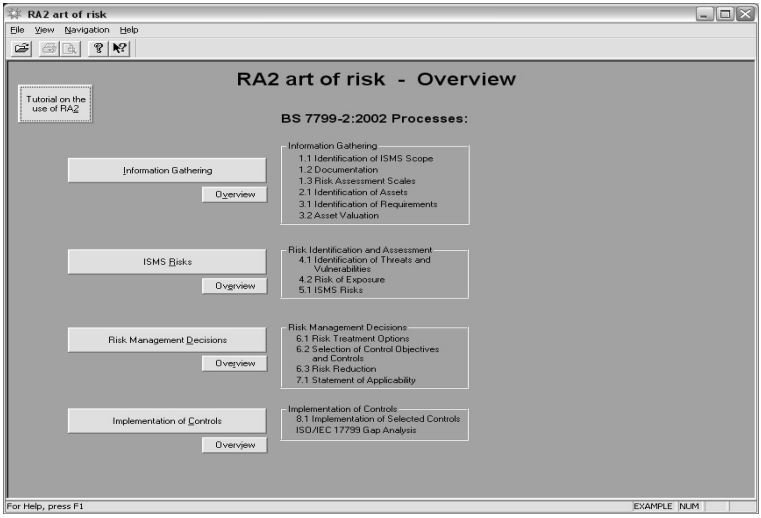
Бұл әдіспен орындалатын тәуекелдерді талдау қауіпсіздіктің базалық деңгейіне жауап береді, яғни тәуекелдер деңгейі анықталмайды. Әдістің артықшылығы – оның қарапайымдылығында. Бірнеше он шақты сұрақтарға жауап беру керек, содан соң есеп беру автоматты түрде құрылады.

Осы программалық өнім ақпараттық қауіпсіздік аудитін жүргізу барысында қолданылуы мүмкін немесе ақпараттардың қауіпсіздігін қамтамасыз етуге жауапты қызметкерлердің жұмысында қажет болуы мүмкін.

Қарапайымдылығы, халықаралық стандартқа сай болуы, басқалармен салыстырғанда сұрақтардың көп емес болуы – осының барлығы бұл әдісті жергілікті шарттарда қолдануға мүмкіндік береді.

RA Software Tool

Базалық деңгейге шартты түрде кіретін тағы да бір әдіс - RA Software Tool - BS 7799 британдық стандарттың 1 және 2-бөлімдеріне, (BSI) PD 3002 британдық стандарттар институтының әдістемелік материалдарына негізделген (тәуекелдерді басқару және талдау әдістемелігі), оның ішінде PD 3003 (BS 7799 стандартына сай кәсіпорынның аудитке дайындығын бағалау), PD 3005 (қауіпсіздік жүйесін таңдау жөніндегі әдістемелік), сонымен қатар ISO 13335 стандартының 3 және 4-бөлімдеріне негізделген (Ақпараттық қауіпсіздік режимін басқару жөніндегі әдістемелік, қауіпсіздікті басқару жүйелері және қауіпсіздікті таңдау шаралары). Әдістің жаңартылған түрінің - RA2 art of Risk - негізгі модульдері 4.2-суретте көрсетілген.



4.2-сурет. RA2 art of Risk модульдері

Бұл құрал-сайман тәуекелдерді бағалауды (4 және 5-модульдар) базалық деңгейдің талаптарына да, PD 3002 британдық институттар стандарттарының жеке спецификацияларына да сай болатындай етіп жүзеге асырады.

Модульдердің әрқайсысы бірқатар қадамдарға бөлінеді. Бұл әдістің көркемделген түрі тәуекелдерді талдау мен басқару туралы өзіндік құрал-саймандарды және әдістемелерді құрғанда керек болады.

CRAMM

1985 жылы Ұлыбританияның телекоммуникациялар және компьютерлер жөніндегі Орталық агенттігі (ССТА) құпия емес, бірақ критикалық мәні бар ақпараттарды өңдеумен айналысатын үкіметтік орындарда қолдануға болатындай ақпараттық қауіпсіздікті талдау әдістерін зерттей бастады. Жоғарыда қарастырылған әдістердің бірде-біреуі сәйкес келмеді. Сол себепті ССТА талаптарын қанағаттандыратын жаңа әдіс ойлап табылды. Ол CRAMM деген атқа ие болды, CRAMM - тәуекелдерді бақылау мен талдаудағы ССТА әдісі. Содан соң Қорғаныс министрлігінің, азаматтық мемлекеттік мекемелердің, қаржылық құрылымдардың, жеке кәсіпорындардың талаптарына негізделген осы әдістің бірнеше нұсқалары пайда болды. Мұндай нұсқалардың бір түрі коммерциялық өнім болып шықты.

Әдісті құрудың мақсаты формализацияланған процедура құру болып табылады, ол келесілерді жүзеге асыра алады:

– қауіпсіздікке байланысты талаптар толығымен талданғанына және құжаттандырылғанына көз жеткізу;

– тәуекелдерді субъективті бағалау кезіндегі мүмкін болатын қауіпсіздіктің артық шараларына кететін шығындарды болдырмау;

– ақпараттық жүйелердің өмірлік циклінің барлық сатыларындағы қауіпсіздіктің жүзеге асырылуына және жобалауына көмек көрсету;

– қауіпсіздіктің талаптарын талдау процесін автоматтандыру;

– қарсы әрекет шаралары үшін негіздемелер келтіру;

– контршаралардың тиімділігін бағалау, олардың әртүрлі нұсқаларын салыстыру;

– есеп берулерді генерациялау.

CRAMM (Internet желісіндегі сілтеуіштер санына қарағанда) тәуекелдерді талдау мен оларды басқарудағы ең кең тараған әдістің бірі болып табылады.

Қазіргі таңда BS 7799 (ISO 27001) стандартына сай CRAMM 5 нұсқасы сатылуда.

Тәуекелдерді талдау қорларға, қауіп-қатерлерге берілген бағалардың негізінде тәуекелдердің деңгейлерін табудан және идентификациялаудан тұрады.

Тәуекелдерді бақылау тәуекелдерді жеткілікті дәрежеге төмендететін контршараларды таңдау мен идентификациялаудан тұрады.

Осы концепцияға негізделген формальды әдіс қауіпсіздіктің барлық жүйені қамтитынына көз жеткізуге мүмкіндік береді және келесілерге сенім арттырады:

– барлық мүмкін болатын тәуекелдер идентифицерленген;

– қорлардың осалдығы идентифицерленген және олардың деңгейі бағаланған;

– қауіп-қатерлердің осалдығы идентифицерленген және олардың деңгейі бағаланған;

– контршаралардың тиімділігі ескерілген;

– АҚ-пен байланысты шығындар ақталған.

АҚ жүйесін зерттеу CRAMM әдісінің көмегімен бірнеше қадамда орындалады. Бірінші қадамда Initiation, ақпараттық жүйенің шекаралары, оның негізгі функциялары, қолданушы категориялары, сонымен қоса зерттеуге қатысатын қызметшілердің формальды сипаттамасы келтіріледі.

Тәуекелдерді бағалау және идентификациялау қадамында Identification and Valuation of Assets, жүйенің қорларының құндылықтарын анықтау мен идентификациялауға байланысты барлық заттар талданады және сипатталады.

Осы қадамның соңында зерттеуге тапсырыс берушінің талаптарын қанағаттандырғанына немесе ол тәуекелдердің толық талдауын өткізуді қажет ететіндігіне көз жеткізеді. Соңғы жағдайда ақпараттық жүйенің ақпараттық қауіпсіздік позициясымен құрылған модель ойлап шығарылады.

Қауіп-қатерлерді бағалау қадамын орындау, Threat and Vulnerability Assessment, міндетті емес, егер тапсырыс берушіні ақпараттық қауіпсіздіктің базалық деңгейі қанағаттандыратын болса. Бұл қадам тәуекелдерді толық талдау жүзеге асырылатын болғанда ғана орындалады. Қорлар тобына арналған қауіп-қатерлердің деңгейін бағалауға және идентификациялауға байланысты барлық шаралар ескеріледі. Қадамның соңында тапсырыс беруші өзінің жүйесіне арналған қауіп-қатерлердің бағаланған және идентифицирленген деңгейлерін алады.

Тәуекелдерді талдау қадамы, Risk Analysis, тәуекелдерді бағалауды не тәуекелдерді толық талдауды жүргізгендегі қауіп-қатерлердің бағаланып қойған нәтижелері негізінде не қауіпсіздіктің базалық деңгейіне арналған қарапайым әдістемеліктерді қолдану негізінде жүргізеді.

Тәуекелдерді басқару қадамында, Risk Management, контршараларды дұрыс іздеу іске асырылады. Негізінде жүйенің қауіпсіздігін қамтамасыз ететін, тапсырыс берушінің талаптарын толығымен қанағаттандыратын нұсқаны табу туралы айтылып отыр. Бұл қадамның соңында ол өзінің жүйесін тәуекелдерден қорғану шараларындағы терминдермен түрлендіру

туралы білетін болады, сонымен қатар қалған тәуекелдерді минимизациялайтын және төмендететін арнайы төтеп беру шараларын таңдай алады.

Әрбір қадам нәтижелерді тапсырыс берушімен талқылап және келіскеннен кейін ғана толығымен бітті деп жарияланады.

CRAMM BS 7799 (ISO 27001) стандартына ақпараттық қауіпсіздіктің сәйкес болатынын тексеру барысында қажетті есеп берулердің генерациялау шараларына ие. Бұл келесі есеп берулер:

– ақпараттық қауіпсіздік саясаты;

– ақпараттық қауіпсіздікті басқару жүйесі;

– тоқтаусыз жұмысты қамтамасыз ету жоспары;

– сәйкестік ведомосі.

Қазіргі таңда CRAMM әдісі жиі қолданылады, көбінесе британдық стандартпен сәйкестікті тексеру жұмысын жүргізу барысында жиі қолданысқа ие.

Оның артықшылығы тәуекелдер мен осалдылықтарды жанама факторлар бойынша бағалау кезінде нәтижелерді верификациялауға мүмкін болатын технологияларды қолануында, ақпараттық жүйені қауіпсіздік жағынан ыңғайлы модельдеу жүйесінің бар болуында, контршаралар бойынша мәліметтер қорының кең болуында болып табылады. Бұл әдіс – қарастырылған шолудың ішіндегі ең «мықты» және ең еңбекқор әдіс, ол өз кезегінде тәуекелдерді толыққанды бағалауға мүмкіндік береді және контршаралардың әртүрлі нұсқаларына баға береді.

Оның кемшілігі, отандық қолданушылардың көзқарасы бойынша, қазақшалау күрделілігінде және шығатын құжаттардың үлкен көлемінде болып табылады. Аналитик (аудитор) әдетте алынған құжаттардың негізінде тапсырыс берушіге есеп берулерді өзі жазуға міндетті.

MethodWare компаниясының программалық жабдықтары

MethodWare компаниясы ақпараттық қауіпсіздік облысында жұмыс істейтін аналитиктер үшін тәуекелдерді талдау, тәуекелдерді басқару жұмысы барысында пайдалы болуы мүмкін бірқатар өнімдер жасап шығарумен айналысады, яғни:

–Тәуекелдерді талдау мен басқару программалық жабдығы Operational Risk Builder және Risk Advisor. Бұл әдістеме Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) австралиялық стандартына жауап береді. ISO 27001 стандартына сәйкес келетін нұсқа да бар;

–Ақпараттық жүйелер облысындағы ашық стандарттармен сәйкес келетін ақпараттық жүйелердің өмірлік циклін басқару программалық жабдығы CobiT Advisor 3rd Edition (Audit) және CobiT 3rd Edition Management Advisor. CobiT әдістемелерінде тәуекелдерді талдау мен басқаруға көп мән беріледі;

– Әртүрлі сұраулар парақтарын автоматты түрде құратын программалық жабдығы Questionnaire Builder.

Risk Advisor ақпараттық қауіпсіздік облысындағы менеджер немесе аналитик құрал-сайманы ретінде орын алады. Ақпараттық қауіпсіздік позициясынан ақпараттық жүйенің моделін құруға мүмкіндік беретін, тәуекелдерді, қауіп-қатерлерді, оқиға нәтижесінде пайда болған шығындарды табатын әдістемелік шығарылды.

Негізгі жұмыс істеу принциптері:

– контексті суреттеу;

– тәуекелдерді суреттеу;

– қауіп-қатерлерді суреттеу;

– шығындарды бағалау;

– басқарушы әсерлерді талдау;

– іс-әрекеттер жоспары мен контршараларды ұсыну.

Бұл кезеңде кәсіпорынның сыртқы ортамен қарым-қатынас моделінің бірнеше аспектілері қарастырылады: стратегиялық, ұйымдастырушылық, бизнес-мақсаттар, тәуекелдерді басқару, сонымен қатар тәуекелдерді бағалау критерийлері.

Стратегиялақ аспектіде кәсіпорынның сырттан қарағандағы күшті және осал жақтары талданады, сонымен қоса кәсіпорынның даму жолдары, қауіп-қатерлер кластары және кәсіпорынның серіктестермен қарым-қатынасы да талданады.

Ұйымдастырушылық контекст кәсіпорынның ішіндегі стратегияларды, ұйымдастырушылық деңгейдегі мақсаттарды, ішкі саясатты белгілейді.

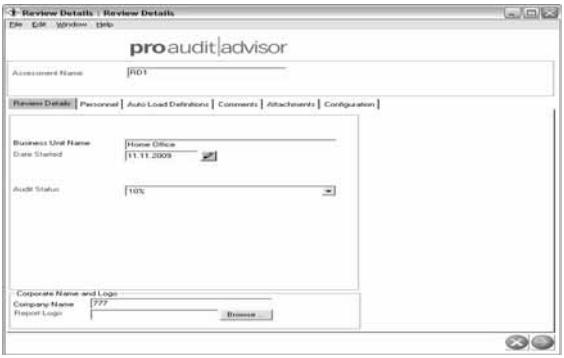
Тәуекелдерді басқару контекстісі ақпараттық қауіпсіздік концепциясын көрсетеді.

Бизнес-мақсаттар контекстісі – негізгі бизнес-мақсаттар.

Тәуекелдерді бағалау критерийі – тәуекелдерді басқару барысындағы қабылданған критерийлер.

Тәуекелдер матрицасы беріледі (4.3-сурет), сондықтан тәуекелдер белгіленген шаблонмен сәйкес суреттеледі және осы тәуекелдер мен модельдің басқа да элементтері арасында байланыс орнатылады.

Тәуекелдер сапалық белгі бойынша бағаланады және қарапайым модель негізінде қабылдауға болатын және қабылдауға болмайтын (4.4-сурет) болып екіге бөлінеді.



4.3-сурет. Risk Advisor тәуекелдерді табу мен анықтау

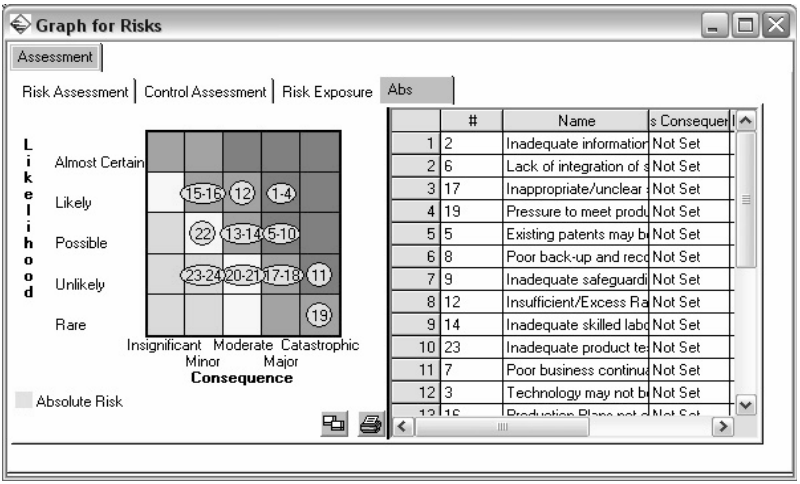
4.4-сурет. Risk Advisor тәуекелдерді қабылдауға болатын және қабылдауға болмайтын етіп бөлу

Содан кейін басқарушы әсерлер (контршаралар) алдын ала бекітілген критерийлер жүйесімен, контршаралардың тиімділік және олардың бағасы жүйесімен сәйкес таңдалады. Тиімділік пен баға сапалы белгілерде бағаланады.

Алдымен қауіп-қатерлер тізімі құрылады. Қауіп-қатерлер белгілі бір түрде классификацияланады, содан кейін қауіп-қатерлер мен тәуекелдер арасындағы байланыс қарастырылады. Суреттеу де сапалы деңгейде іске асырылады және байланыстарды бекітуге мүмкіндік береді.

Ақпараттық қауіпсіздік режимін бұзумен байланысты оқиғалар (зардаптар) тізімі келтіріледі. Шығындап таңдалынған критерийлер жүйесінде бағаланады.

Модельді құру нәтижесінде толық есеп беруді шығаруға болады (шамамен 100 бөлім), экраннан агрегатты суреттеуді тәуекелдер графигі түрінде көруге болады (4.5-сурет).



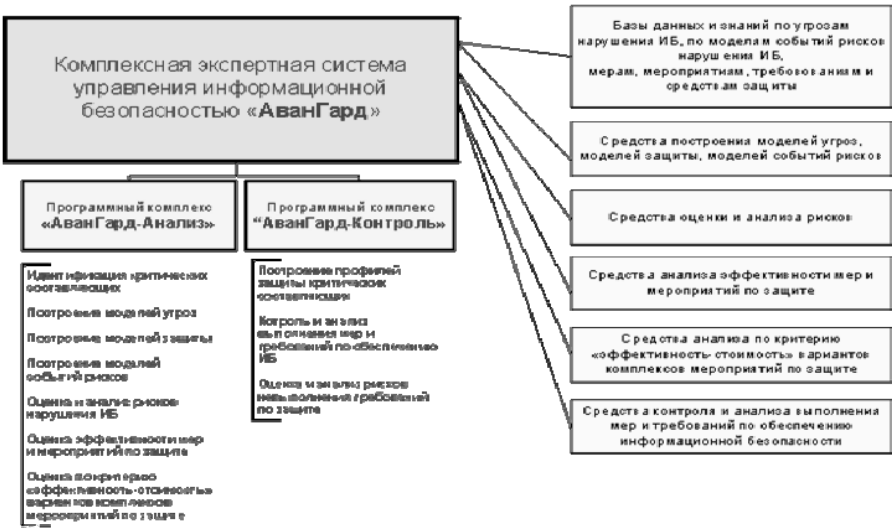
4.5-сурет. Risk Advisor нәтижелерді талдау

Бұл құрал жоғарғы деңгейлердегі - басқарушылық және ұйымдастырушылық – тәуекелдерді басқарумен байланысты барлық мүмкін болатын аспектілерді құжаттандыруға мүмкіндік береді. Ал программалық-техникалық аспектілерді белгілеу бұл модельде онша ыңғайлы емес. Бағалар сапалы белгілер түрінде беріледі және тәуекелдердің факторларын толық талдауы ескерілмейді.

Бұл әдістің мықты жағы өзара байланыстарды түрлі жоспарлар түрінде көрсету мүмкіншілігі бар, тәуекелдердің көптеген факторларын адекватты түрде тіркеу және CRAMM әдісімен салыстырғанда жұмыс көлемі аз болып келеді.

«АванГард» экспертті жүйесі

Қазіргі таңда Ресейде РАН жүйелік талдаудың Институты құрып шығарған «АванГард» программалық жабдығы сатылуда. «АванГард» ақпаратты қауіпсіздікті басқару жүйесі ретінде сипатталады. Бұл жүйенің құрылымы мен атқаратын қызметтері 4.6-суретте көрсетілген.



4.6-сурет. «АванГард» құрылымы мен функциялары

Программалық құралдардың типтік пакеті КЭС «АванГард» екі программалық жиыннан тұрады: «АванГард-Талдау» және «АванГард-Басқару». Осы жиындардың әрқайсысы өзінің тәуекелдерді талдау әдістемелігіне сүйенеді.

Бірінші жиында, яғни «АванГард-Талдау», бағаланатын жүйенің тәуекелдерді құратын потенциалды компоненттерін есептеу негізінде тәуекелдерді бағалау жүзеге асырылады. Бұл жерде тәуекелдерді құратын потенциал ұғымы ретінде осы компонентке кіретін жүйемен байланысты қосынды тәуекелдің бөлігі түсініледі. Тәуекелдерді құратын потенциалдарды есептеу келесі түрде жүргізіледі.

Алдымен құрамында мүмкіндігінше толық оқиғалардың формальды емес анықтамалары мен осы оқиғаларға әкеліп соқтыратын тәуекелдер тізімі бар модельдер құрылады. Содан соң тәуекелдердің оқиғалар модельдерінің әрқайсысы бойынша тәуекелдің бағалануы жүргізіледі, яғни тәуекел оқиғасының болу ықтималдығын бағалау және тәуекел оқиғасының қауіп-қатерінің деңгейін бағалау туындысы есептеледі. Бұған қоса бағалауларды, яғни тәуекел оқиғаларының ықтималдықтары мен осы оқиғалардың қауіп-қатерінің деңгейінің бағалауларын рангілік өлшемдердің көмегімен алу керек. Ықтималдықтар өлшемінің 0-ден 100-ге дейінгі бекітілген өлшем бірлігі бар (0-ден 100-ге дейінгі тәуекел оқиғасының бір жыл аралығындағы пайда болуының проценттік ықтималдығы). Қауіп-қатерінің өлшемінің төменгі шегі - 0, ал жоғарғы шегі жоқ,

сондықтан қауіп-қатерінің өлшемі келесі түрде құрылады. Алдымен оған барлық қауіп-қатерлер материалды шығындарға әкелетін және ақшалай түрде болуы мүмкін тәуекелдер енгізіледі. Мұның нәтижесінде тәуекелдер оқиғаларының қауіп-қатерлерінің базалық өлшемі құрылады. Содан кейін қолданушыларға «ақшалық» метрикадан алшақтап, өлшемді жеке оқиғалардың қауіп-қатерлерінің қатысты деңгейі ретінде ғана түсіну керек екендігі ұсынылады және өлшемге тәуекелдер оқиғаларының қажет еместігінің немесе болдырмауының деңгейлерін салыстыру арқылы көрсету керек екендігі жайлы ескеріледі. Осыған қоса өлшемнің жоғарғы шегі талаптарға байланысты көтерілуі мүмкін. Жіберілген бағалаулардың ықтималдықтар мен әрбір көрсетілген тәуекел оқиғасының қауіп-қатерінің деңгейін алдын ала анықталған деңгейлермен салыстыру арқасында мықты верификациялау механизмі анықталады. Егер қандай да бір жұп үшін бағалаудағы қатынас эксперттер көзқарастарына сай келмесе, онда ертерек қойылған бағалаулар қайта қаралуы тиіс. Сонымен қатар қойылған бағалауларды баспадан шығару мүмкіндігі және оларды көптеген эксперттердің көмегімен талқылау мен түзету мүмкіндіктері ескерілген.

Бұл әдістемелік кез келген тәуекел оқиғасы белгілі бір қауіп-қатерлер жиынының орындалуы барысында жүзеге асады, олардың әрқайсысы өз кезегінде бағаланатын жүйенің қандай да бір компонентінің қауіпсіздігінің қауіп-қатері ретінде анықталуы мүмкін. Бұның арқасында әрбір қауіп-қатердің оның тәуекел оқиғасына «құрамы» негізінде тәуекел құру потенциалын, осы қауіп-қатерлер кіретін компоненттердің тәуекел құру потенциалдарын да анықтауға болады және бағаланатын жүйе мен толық жүйенің барлық құрылымды құраушылары бойынша тәуекелдерді есептеуге болады.

Сонымен қатар құрастырушылармен ұсынылып отырған «Аван-Гард-Талдау» программалық кешені АҚ басқаруға байланысты есептеулерді шешуде қосалқы рөл атқаруға бағытталған, яғни: қауіпсіздіктің мақсаттарының жиынтығын дұрыс қисынға келтіруге мүмкіндік беретін жанжақты толыққанды талдауды қамтамасыз етеді, қауіпсіздік саясатын негіздейді, қауіпсіздіктің барлық талаптарын орындауда кепілдік береді. Сәйкесінше ондағы тәуекелдерді бағалау көрсетілген мәселелерді шешу мақсатымен жүргізіледі.

«АванГард-Басқару» кешенінде тәуекелдерді бағалау әдістемесі АИСтің қорғаныс деңгейін бақылайтын шартқа негізделгендіктен оның әдістемесі «АванГард-Талдау» кешенінен өзгеше болып келеді. Егер «АванГард-Талдау» кешенінің әдістемесі бағаланатын жүйенің қауіпсіздігінің бұзылуының тәуекелдеріне қатысты болса, онда «АванГард-Басқару» кешені бағаланатын жүйенің және оның компоненттерінің қауіпсіздігін қамтамасыз ету бойынша талаптардың орындалмағандығына байланысты болып табылады.

Осыдан шығатын қорытынды, «АванГард-Басқару» жүйесін қолдану үшін, бағаланатын әрбір жүйе үшін толық талаптар құрамы болуы қажет, олардың орындалуы жүйе қауіпсіздігінің бұзылу қаупі өте аз екендігін білдіреді. Сонымен қатар егер барлық талаптар дұрыс орындалмаса, жүйе қауіпсіздігінің бұзылу қаупі 100 пайызды құрайды.

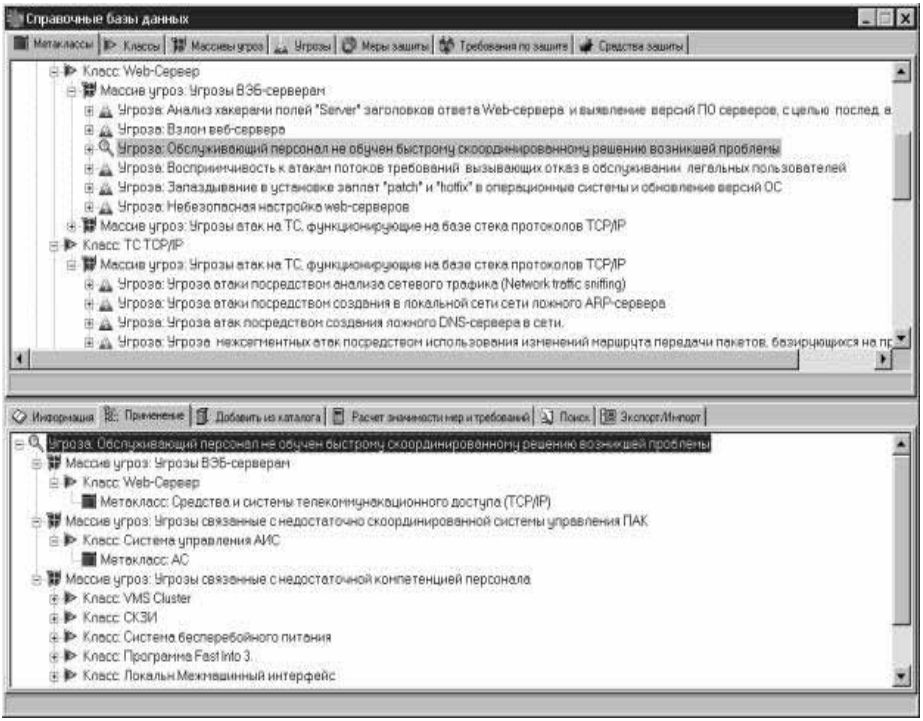
Толық талаптар құрамын құру бойынша жұмысты жеңілдететін бір шарт бұл 2002 ж. ақпараттық технологиялардың қауіпсіздігін басқаратын критерий бойынша жасалған ГОСТ Р ИСО/МЭК 15408-2002 жүйесінде қорғаныс профилін бағаланатын жүйенің жекелеген компоненттеріне қолдануға мүмкіндік береді. Бұл ГОСТ 2004 ж. іске қосылатындығын ескере отырып, оның талаптарын орындамаудан шығатын тәуекелдерді «АванГард-Басқару» жүйесі арқылы бағалауды қарастырып өткен жөн.

Алдын ала айта кететін жайт, «АванГард-Басқару» жүйесі екі бөліктен тұрады: «АванГард-Орталық» программалық кешенінен (ПК) және «АванГард-Аймақ» программалық кешенінен (ПК). Біріншісі бірнеше мақсаттарды көздейді, олар: қорғаныс профильдерін құру; АИС басқару бөліктеріне электронды пошта арқылы қорғаныс профильдерін жеткізу; АИС бөлімдерінде қауіпсіздік талаптарының орындалғандығы жөнінде есептерді автоматты түрде жинау; АИС-те қауіпсіздік талаптарының орындалмауының тәуекелдігіне баға беру; қорғаныстағы кішігірім орындарды анықтау. Екіншісі – АИС-тің жекелеген бөлімдерінде қорғаныс профилін алу; қорғаныс профилінің талаптарын орындалуы жөніндегі есептерді бақылау және сол есептерді қайта қарау үшін ПК «АванГард-Орталық»-қа жіберу.

ПК «АванГард-Орталық»-та қорғаныс профильдерін дамыту программалық кешеннің каталогтар бөлімінде іске асады. Бастапқыда ПК «АванГард-Орталық» жүйесінде бірнеше маңызды түсініктемелер қалыптасқан, олар: метакласс, класс, шара, талап. *Метакластар* АИС объектілерінің кластарын нақтылы бір белгілер бойынша топтауға бағытталған. *Кластар* белгілі бір талаптар құрамы (қорғаныс профилі) белгіленген, объектілер кластарын құрайды. *Шаралар* ГОСТ Р ИСО/МЭК 15408-2002 түсініктемесіне қойылатын функционалды кластар мен талаптар кепілдігі кластарын белгілейді. *Талаптар* құрамына ГОСТ Р ИСО/МЭК 15408-2002 сай функционалды жүйелер, кепілдік жүйелері, функционалды компоненттер, кепілдік компоненттері, функционалды элементтер және кепілдік элементтері кіреді.

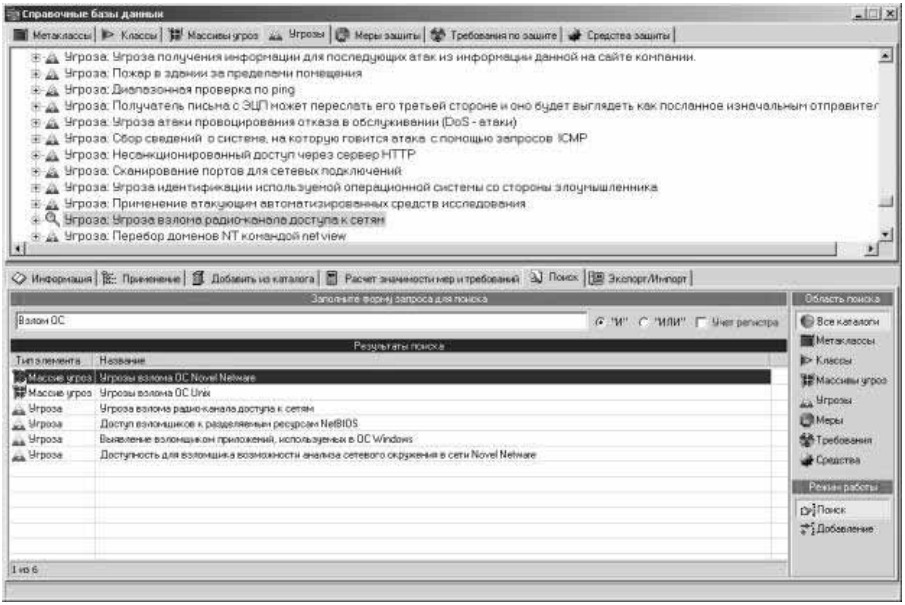
ГОСТ Р ИСО/МЭК 15408-2002 негізінде жасалған қорғаныс профильдері үшін ПК «АванГард-Орталық» каталогтарында «ГОСТ Р ИСО/МЭК 15408-2002-ге бағытталған талаптар мен қорғаныс профилі» атты метакласс бөлек көрсетілген (4.7-сурет). Осы метакласта бір «негізгі» класс құрылған, онда ГОСТ Р ИСО/МЭК 15408-2002-де қарастырылған барлық талаптар дерлік қамтылған, олар функционалды және қауіпсіздік кепілдік-

теріне қатысты болып табылады (4.8-сурет). Әр деңгей бойынша форманың оң жақ төменгі жағында толық ақпарат жазылады, ол ақпарат таңдап алынған каталогқа сай болу керек. 4.9-суретте ПК «АванГард-Орталық»-тағы талаптар жиынтығы көрсетілген. Қарастырылып отырған мысалда FAU_GEN.1 талаптар тізімін анықтау үлгісінен, мұндай үлгілер әрбір қорғаныс профиліне сай өзгеретіндей жүйеге ауыстырылған. ГОСТ Р ИСО/МЭК 15408-2002 бойынша қорғаныс профильдері төмендегідей жүзеге асады. ПК «АванГард-Орталық» әдістері арқылы «ГОСТ Р ИСО/МЭК 15408-2002 талаптары» атты кластың көшірмесі жасалады. Содан соң «қорғаныс профилінің шаблоны ретінде қою» операциясы «ГОСТ Р ИСО/МЭК 15408-2002-ге бағытталған талаптар мен қорғаныс профилі» дегенге қолданылады.



4.7-сурет. «АванГард-Орталық»-тағы метакласс құрамы

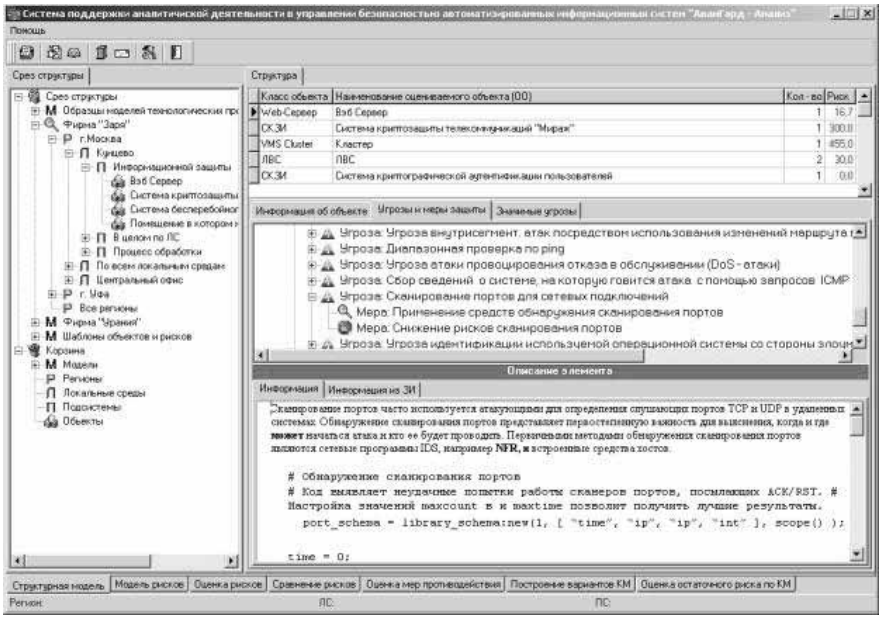
4.8-сурет. «АванГард-Орталық»-тағы «класс» құрамы



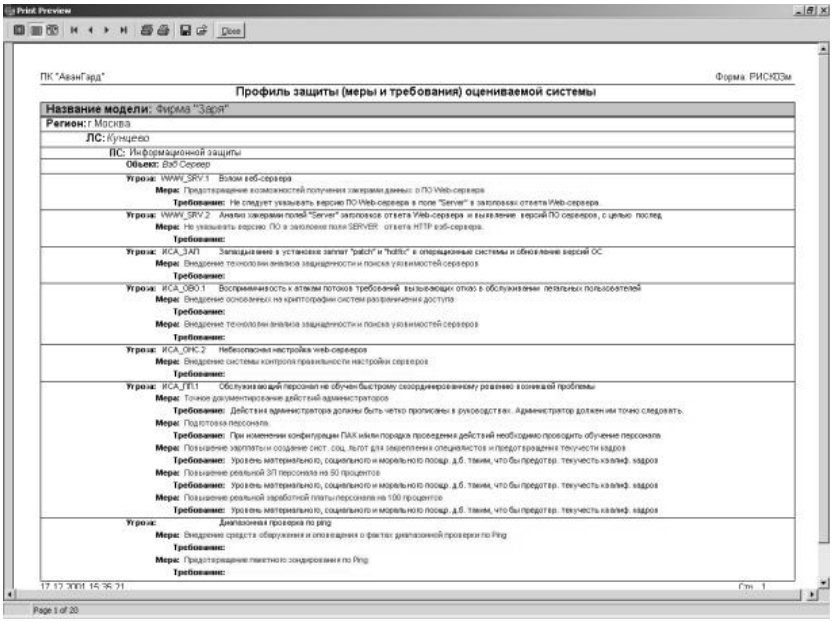
4.9-сурет. ПК «АванГард-Орталық»-тағы талаптар құрамы

Сонымен қатар кластың атауын өзгерту ұсынысы да бар. Сол атауы: «Қолжетімділікті бөлу жүйесі – Қорғаныс профилі» дегенге ауыстырылды делік. Соның нәтижесінде болашақ талаптарды ескеретін шаблон құрылады, ол бойынша соңында осы қорғаныс профилі құрылып жатқан объектілердің қорғаныс талаптарына жауап беретін шаралар ғана қалады (4.10-сурет). Бұл профильде қажеті жоқ барлық талаптар мен шаралар жойылады да, қалғандары нақты объектінің қауіпсіздігін қамтамасыз етуге бағытталған талаптарға сай өзгертіледі.

Қарастырылған мысалда шаблон ретінде ГОСТ Р ИСО/МЭК 15408-2002 толық талаптары қолданылған, алайда жаңа профиль құру үшін дайын қорғаныс профильдері де шаблон бола алады, сонымен қатар одан қажеті жоқ шаралар мен талаптарды жою ғана емес, қажет жағдайда жаңа шаблондар енгізіп, жаңа қорғаныс профиліне қажетті қауіпсіздік талаптарына жауап беретіндей деңгейге жеткенше өзгертуге болады. Құрылған қорғаныс профильдерін қағазға басып шығаруға да немесе WinWord форматындағы редакторға да жіберуге болады. Іске асырылатын есептің бір бөлігі 4.11-суретте көрсетілген.



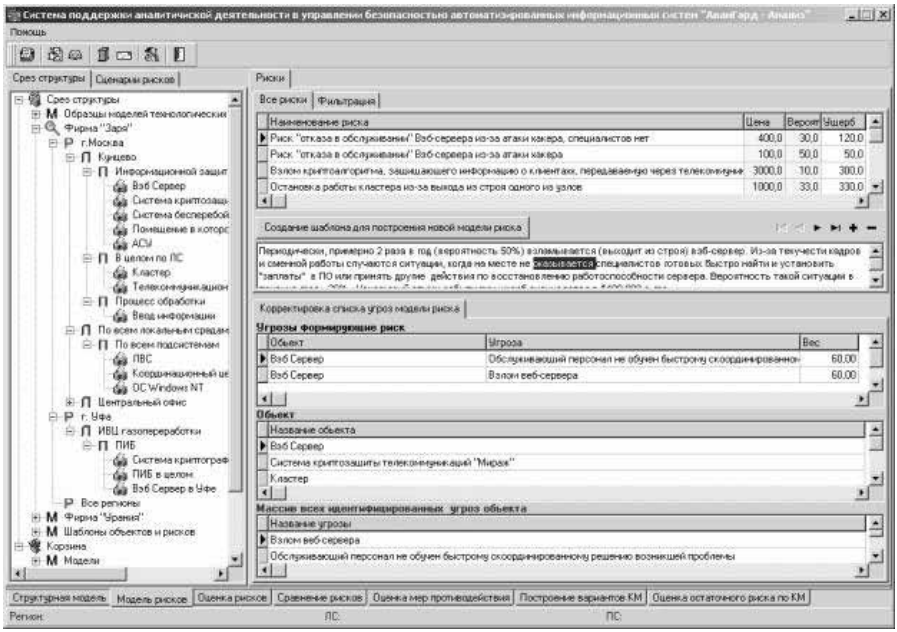
4.10-сурет. Қорғаныс профилі



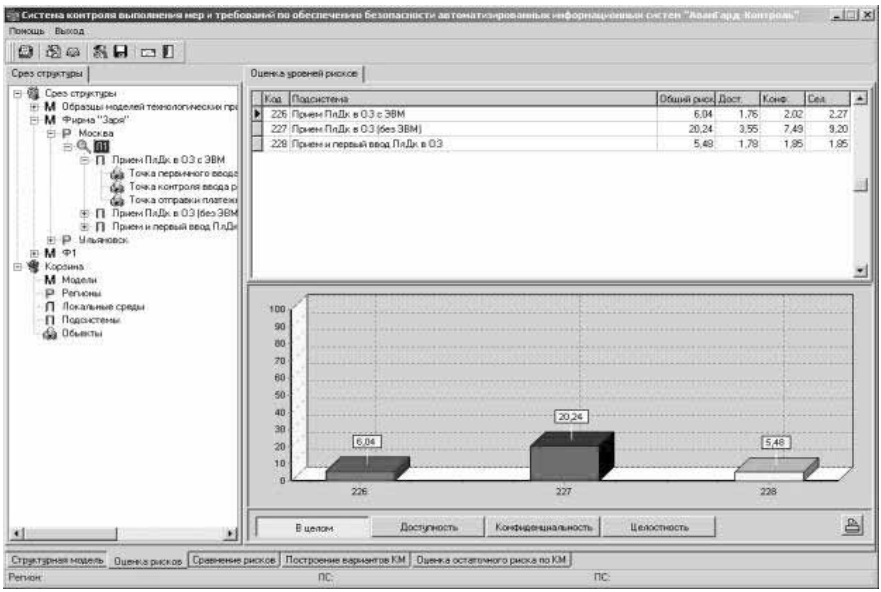
4.11-сурет. ПК «АванГард-Орталығы»

ПК «АванГард-Орталық» жүйесі негізінде жасалатын белгіленген қорғаныс профилі арқылы бағаланатын объектілер құрылымдық жүйеден сарапталатын жүйеге өте алады. Бұндай баға беру объектілерін құру үшін анықталған қорғаныс профилінің қауіпсіздік талаптарына жауап беретін элемент ретіндегі модельге керекті қорғаныс профилін тасымалдауға болады. Жекелеген орындалған талаптарды бекіту жөніндегі фактілерді көрсететін, осындай операциялар мен баға берудің нәтижесі 4.12-суретте көрсетілген.

«АванГард-Орталық» жекелеген баға беру объектісіне қатысты профильді қорғаныс талаптарының орындалуына жасалған сараптама нәтижесінде ақпараттық жүйеде талаптардың орындалмауының тәуекелдерін бағалауға мүмкіндік береді. Талаптарды орындамағанның тәуекелдерді бағалау гистограммасы 4.13-суретте мысал ретінде көрсетілген. Неғұрлым көп талаптар орындалмаса, соғұрлым тәуекелдер көлемі артып, гистограмма бағаны жоғарылайды. Қарастырылған мысалда жеке талаптардың маңыздылығы бірдей деңгейде қабылданған, алайда баға беру объектісінің қауіпсіздігін қамтамасыз етуге бағытталған жеке талаптардың маңыздылығын ескеретін әртүрлі мағыналар беруге болады.



4.12-сурет. Белгілі бір нақты бағаланатын объектіде қорғаныс профилі



4.13-сурет. «Авангард-Орталық»-та бағасының графикалық сипаттамасы

Осылайша, КЭС «АванГард» ГОСТ Р ИСО/МЭК 15408-2002 негізінде қорғаныс профильдерін жасап шығару қадамын автоматтандыруға ғана емес, сонымен қатар қорғаныс профилін ұйымның ақпараттық жүйесіне қойылатын талаптарының орындалуына баға беру үшін де қолдануға болады.

Қорыта келгенде, «АванГард» сараптамалық жүйесі қауіптерді сараптау мен оларды басқаруда ведомствоаралық және корпоративті әдістер құру үшін тиімді болып табылады. Оны қауіптерді бағалау мен сараптау үшін қолданылатын мықты құрал-сайманы ретінде қарастыруға болады және де АИС-тің қауіпсіздігін жүйелі түрде бақылаудың мақсаттарын шешу рөлін де АИС-ті қолданатын барлық бөлімдерде атқара алады (оның ішіне мынадай топтарды жатқызады, олар қауіпсіздік саясатын жүргізу, ГОСТ пен Мемтехкомиссияның шарттары, қауіпсіздікке қатысты заңнамалық актілер, ішкі бұйрықтар мен шешімдер).

RiskWatch

RiskWatch компаниясы екі өнімді ұсынады: біреуі ақпараттық, екіншісі физикалық қауіпсіздікке қатысты. Программалық жабдық кәсіпорынның компьютерлік және физикалық қауіпсіздік саласындағы қорғалынатын қорларды, қауіп-қатерлерді, осалдылықтарды идентификациялау мен бағалауға арналған.

Ақпараттық тәуекелдерді басқаруға арналған өнімде АҚШ стандартына қойылатын талаптар ескеріледі (қорғаныстың қажет деңгейін таңдауға болады). Сонымен қатар ISO 27001 стандартына сай келетін RiskWatch RW27001® өнімінің түрі қолданысқа енгізілді. RiskWatch тәуекелдерге сараптама жасап, қорғаныстың түрлері мен тәсілдерін таңдауға мүмкіндік береді. Программада қолданылатын әдістеме төрт қадамнан тұрады.

Бірінші қадам – зерттеудің пәнін анықтау. Осы қадамда ұйымның параметрлері сипатталады: оның түрі, зерттелетін жүйенің құрамы, қауіпсіздік саласындағы негізгі талаптар (4.14-сурет). Сипаттама бірқатар қосымша пунктерде көрсетіледі, оларды мейлінше нақтылау (4.15-сурет) үшін ескерсе де болады немесе жібере салу да көзделген.

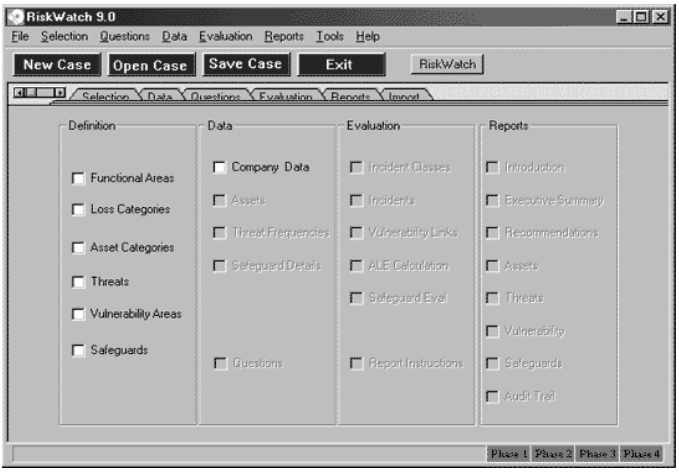
Одан кейін әрбір көрсетілген пункт нақтылы сипатталынады.

Сарапшының жұмысын жеңілдету үшін шаблондарда қорғалынатын қорлардың, қауіп-қатерлердің, осалдылықтардың категорияларының тізімі мен олардан қорғану әдістері көрсетіледі. Солардың ішінен өндірісте шынымен орын алғандарын таңдап алу керек.

4.15-суретте қорлардың әртүрлі категорияларының сипатталуының мысалы келтірілген.

Атаулар мен сипаттамалардың түрлендірулері де қолданылады, сонмен қатар осы әдісті жеңіл русификациялау үшін жаңа категорияларды енгізуге болады.

Екінші қадам – жүйенің белгілі бір сипаттамаларына байланысты бар ақпараттарды енгізу (4.16-сурет). Ақпарат қолдан немесе компьютерлік жүйелердің осалдығын тексеру кезіндегі программалық жүйелермен жасалған есептер арқылы енгізіледі.



4.14-сурет. Ақпараттық жүйені RiskWatch-тағы қауіпсіздік деңгейінен сипаттау

Бұл қадамда:

– оқиғалардың қорлары, класстары және шығындары толығымен сипатталған. Оқиғалардың кластары шығын мен қорлардың категорияларын теңестіру арқылы анықталады;

– 600 сұрақтан тұратын сауалнама негізінде бар кемшіліктерді анықтауға болады. Сұрақтар қорлар категорияларына байланысты. Онда түзетулерге және сұрақтарды алып тастауға немесе жаңа сұрақтар қосуға мүмкіндік беріледі;

– әр анықталған қауіптің пайда болуының ұзақтығы, әсер ету деңгейі және қорлардың құндылығы белгіленеді. Осының барлығы болашақта тиімді қорғаныс шараларын енгізу үшін қолданылады;

Үшінші қадам – тәуекелдерді бағалау (4.17-сурет). Алдымен алдыңғы қадамдарда анықталған қорлар, шығындар, қауіп-қатерлер және осалдықтар арасында байланыс орнатылады.

Тәуекелдер үшін $m = p \times v$, формуласы арқылы бір жылдық шығындар математикалық тұрғыдан есептеледі.

4.15-сурет. Ақпараттар жүйесінің қорлар сипаттамасы

Мұнда p – бір жыл ішінде қауіптің пайда болуының ұзақтығы, v - қауіпке шалдыққан қорлардың бағасы.

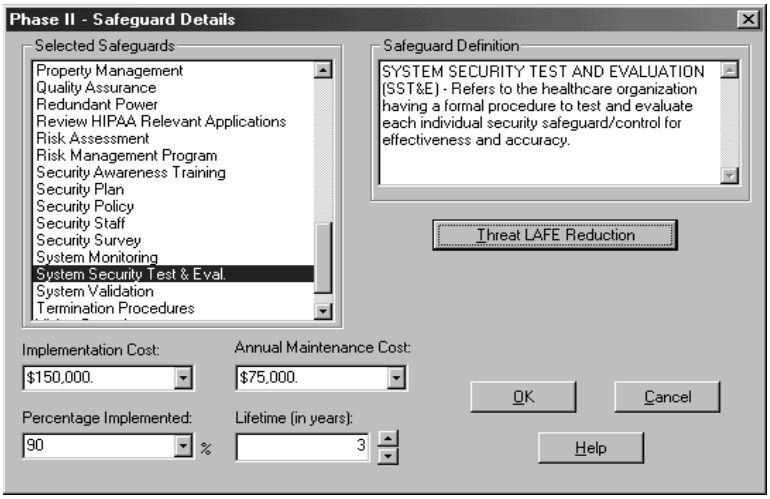
Мысалы, егер сервердің құны 150 000 долл. құраса, ал оның бір жыл ішінде өртке шалдығу мүмкіндігі 0,01 болса, онда күтілетін шығындар 1500 долл. бағаланады.

Қосымша «егерде» деген нұсқа да қарастырылады, мұндай нұсқа қорғаныстың әдістерін енгізудің негізінде ұқсас оқиғаларды сипаттауға мүмкіндік береді. Күтілетін шығындарды қорғаныс әдісі болсын-болмасын теңестіру арқылы осындай іс-шаралардың нәтижесін бағалауға болады.

Төртінші қадам – есеп беруді генерациялау. Есеп берудің түрлері:

- қысқа мерзімді нәтижелер;
- 1 және 2-деңгейлерде сипатталған элементтер жайлы толық және қысқа мерзімді есеп берулер;
- қауіп-қатерлерді анықтау барысында күтілетін шығындар мен қорғалатын қорлардың құны туралы есеп беру;
- қауіп-қатерлер мен оларға қарсы тұру шаралары жөнінде есеп беру;
- қауіпсіздік аудитінің нәтижелері жөнінде есеп беру;

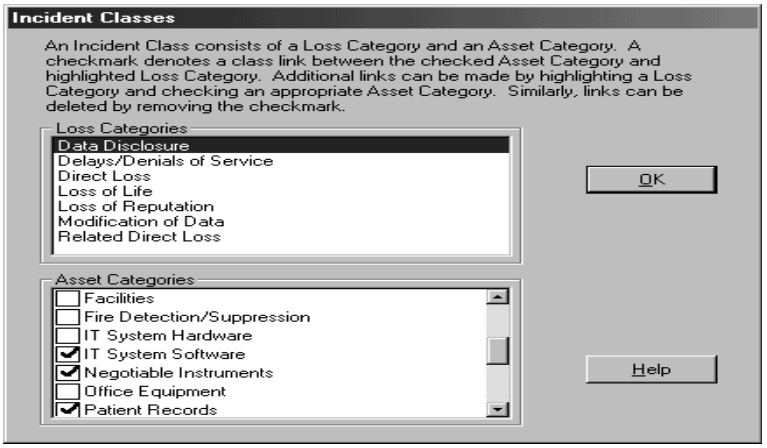
Төменде (4.18-сурет) есеп берудің бөлігі көрсетілген.



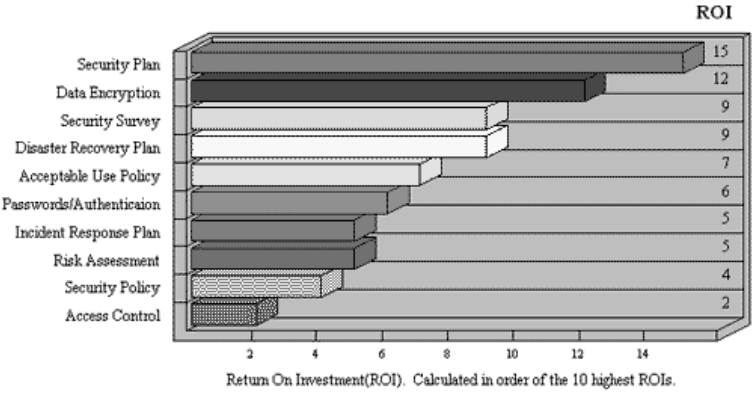
4.16-сурет. Статистикалық мәліметтерді қолдану арқылы қауіп-қатер параметрлерін анықтау

RiskWatch-та жеңілдетілген әдіс ақпараттық жүйенің моделін сипаттау үшін және тәуекелдерді бақылау үшін қолданылады.

Осы әдіс арқылы тәуекелдерді бақылау бойынша жүргізілетін жұмыс көлемі онша да үлкен емес. Тәуекелдерді бақылау бойынша қауіпсіздікті техникалық-программалық деңгейде ұйымдастырушылық және әкімшілік факторларды ескермей жүргізсе, бұл әдіс өте тиімді болып табылады. Алайда ескере кететін бір жайт, алынған тәуекелдердің бағасы (күтілетін математикалық шығындар) тәуекел ұғымын жүйелік тұрғыдан жоққа шығармайды. Отандық тұтынушының көзқарасы бойынша RiskWatch-тың негізгі жағымды жақтарына келесілерді жатқызуға болады: салыстырмалы жеңілдігі, русификациялау кезіндегі жеңілдіктер, әдіске жаңа категорияларды, сипаттамаларды, сұрақтарды және т.б. енгізуге болатындай тиімділігі. Осы әдістің негізінде отандық құрастырушылар қорғаныс саласындағы отандық талаптарға сай өздерінің профильдерін құрастырып, ведомствоаралық тәуекелдерді бақылау мен басқару әдістемелерін жасап шығара алады.



4.17-сурет. RiskWatch-тағы үшінші деңгейдің мазмұны



4.18-сурет. Қауіп-қатердің бірі – тоңаудың (басы) нәтижелік бағалары

V ТАРАУ

ҚАУІПСІЗДІК ТЕКСЕРІСІ ЖӘНЕ ТӘУЕКЕЛ

5.1 Қауіпсіздік тексерісінің өзектілігі

"Ақпараттық аудит қауіпсіздігі" деген бізде аз ғана уақытта пайда болды. Қазіргі заман талабына сай бірлескен жүйедегі ақпараттық аудит қауіпсіздігінің қарқынды және көкейкесті стратегиялық дамуына тез арада қызушылығын арттыруда. Ақпараттық қауіпсіздік – сол компанияның көкейкесті мәселесі, алға қойылған мақсаты мен экономикалық мүддесінің жағдайын жүзеге асыру. Корпоративтік жүйедегі АҚ жіберген кемшіліктер мен жеткен жетістіктерін бағалауды көрсеткіштер арқылы біледі.

Білімділігімен және жоғары деңгейде жүргізілген аудит арқылы АҚ ұжымның күнделікті жұмысымен бизнес мақсатын бірлескен жүйеде құруға болады.

Компания үшін аудит қауіпсіздігі тиімді ме?

Жасыратыны жоқ, көп компанияларда бірлескен жүйе арқылы қорғау көптен байқалады. Бұл компанияның қызметінің ұлғаюы бірлескен жүйеде жіктеледі. Сондықтан бұл жүйеге құнды құжаттар бөлініп отырады. Соған орай ақпараттық жүйедегі аудиттің көкейкесті өзектілігі ақпараттық қауіпсіздікті көбейтеді.

Бірлескен ақпараттық жүйенің қалыптасқан түрінде салынған қаражатты компания ойдағыдай жұмсай алмайды. Өйткені бірлескен жүйенің өзінің де осал жерлері бар.

Бірлескен жүйенің екі түрлі осал жерін атап өтуге болады. Біріншіден, ақпараттық жоба элементінің қиындатылуы, жаңа технологияларды өңдеу, оның құрылымдары мен функционалды қиындықтары мен күрделенуі және жүйелердің тапсырысы мен сақталуының салдарынан болады. Екіншіден, заман талабына сай өнеркәсіп өндіргіштер мен ашық бәсекелестіктің көбеюіне байланысты "ақпараттық соғыстардың және электрондық диверсиялардың" осы саладағы істі жетік білетіндердің бәсекесінен туындап отыр.

Осы заманғы АҚ-ті өте көп және әртүрлі ақпараттық жағдайда қорғауға болады. АҚ-ті жаңа жобалар мен жаңа үрдістер арқылы жаңартып отыру керек.

АҚ-ті ұдайы жаңартып отырудың екі тәсілі бар: біріншісі – үлкен қаражат жұмсай отырып АҚ-тің қорғаныш жүйесін толығымен ауыстыру.

Екінші түрі – модернизацияны өзгерту. Соңғы түрі, яғни модернизацияға қаражат аздау кетуі мүмкін. Бірақ оларды ауыстырған кезде жаңа қиындықтар туындауы мүмкін, өйткені бұрынғы ескі қалыптасқан ақпарат жүйесін жаңалау арқылы қауіпсіздігін сақтау керек. Әр текті құралдармен орталықтандырылған басқаруды ұйымдастыру және оның қауіпсіздігін қалай үйлестіруге болады? Керек болған жағдайда компанияның ақпараттық тәуекелін қалай жаңалап, бағалап білу керек? Қауіпсіздікті тексеру мына жағдайда керек, модернизация мен жаңа технология кезінде толық іске аспағанда, сол кезде қауіпсіздік тексерісі мынадай жағдайларда талдап бағдар береді: бағалау, тәуекелге бел буу, компанияның бизнестік бағдарламасын, ақпараттық актив-стратегиялық жоспарын, маркетингтік жобасын, бухгалтерлік және финанстық ведомстік бірлескен базасын түсіндіреді. Қорытындысында сауатты жүргізілген ақпараттық қауіпсіздігін тексерудің арқасында АҚ жүйесінде үлкен мақсатқа жетуге болады.

АҚ менеджмент пен бірлескен жүйеде АҚ-ні тексеруі командамен жұмыс істейді. Әртүрлі ағымдағы маман иелерінің көзқарасын компанияның АҚ-ға бағыттайды. Барлығы бір командаға бірігіп, осы компанияның экономикалық және рентабельді ұтымды бизнесін жүргізеді. АҚ аудитінің тағы бір қосымша жағдайы бар, ол корпоративтік қауіпсіздік ақпаратты анализдап, талдау жасайды. Анализдер мен CASE орталығы құрылымдық бағыт-бағдар басқаруына әртүрлі бағытта ақпарат жүйесіне көрнекті және маңызды баға береді. Мұндай қорытынды баға беру компанияның ақпараттық инфрақұрылымын айрықша графикалық түрде білдіреді.

Осы әртүрлі уақытта көптеген ұйымдар толық ақпараттық қауіпсіздік бағдарын ұсынады, өкінішке орай осыған байланысты ыңғайланған жобаға келіп тірелеміз.

Корпоративтік жүйенің қауіпсіздігі “көлеңкеде” қалып қояды. Сондықтан ТОР менеджерлер мынадай сұраққа келіп тіреледі:

- Корпоративтік жүйе АҚ осы компанияның мақсаты мен бизнесіне лайық па?
- Компанияның қауіпсіздік саясаты мен кәсіпкерлік мақсаты сай келе ме?
- Қауіпсіздік саясаты мен оның орындалуы нәтижелі бола ма?
- Модернизациялауды қалай өткізуге болады?
- Жаңарту негізіндегі шығынды қалай негіздеу?
- Қауіпсіздік бірлескен жүйенің шығынын қалай тез ақтайды? Зардабы болмайтын жақтарын қалай қарастыру?
- Штат кестесі қауіпсіздік жағдайын дұрыс жүргізуге арналған ба?
- Компанияның қорғаныш құралдары – желі аралық экрандық (firewall), басып ену (IDS) вирусқа қарсы шлюз VPN-шлюзы, жұмыстарын табанды түрде атқара ала ма?

- Бағдарламалардың тарап кетпеуі, жасырын түрде болуы шешілген сұрақтар ма?

- Компанияның құрылымын жеткізу, монтаж жасаған ұйымның жұмыстарын қалай бағалауға болады? Кемшіліктері болса, қандай деген сұрақ туады.

- Орталықтандырылған қауіпсіздігін қалай жасауға болады?

- Компанияның АҚ қалай бақылауға алуға болады? Қандай амал қолдануға болады?

- Компанияның бірлескен қауіпсіздік жүйесін құрып болған соң әрі қарай не істеуге болады? (Оның тактикалық және стратегиялық төтенше жағдай кезіндегі амалдары)

- Копанияның АҚ қызметкерлерін әрдайым үйретіп отыру керек пе? Керек болған жағдайда оған жұмсалар қаражат көлемі қандай?

- Ақпараттық тәуекел жұмысын қалай басқаруға болады? Оны қандай құрал-жабдықтармен жүргізуге болады?

- АҚ ұйымы халықаралық бағалау стандарттар мен қауіпсіздік басқармасының талаптарын қанағаттандыра ма? Мысалы, ISO 15408, ISO 27001 (BS 7799), BSI?

Туындаған сұрақтарға бірден жауап бере алмайтынымыз айқын. Тек қана бірлескен жүйенің объективті және тәуелсіз қауіпсіздік аудиті сауатты, анық ақпарат береді. Мұндай аудит АҚ компаниясының негізгі қамтамасыз ету деңгейлері тексереді: нормативті заңды, ұйымдық, технологиялық және аппараттық-бағдарламалық.

КИС-тің қауіпсіздік деңгейіне қалай баға беруге болады?

Қазіргі уақыттағы ақпараттық жүйенің тәуекелді талдау әдістемелері, қауіпсіздік жүйесінің жобалауы мен әрі қарай жұмыс істеу мүмкіндіктері мыналарды туғызады:

- Ұйымдық-басқарылымдық, технологиялық және техникалық деңгейлерде сандық бағалаудың ағымдағы деңгейін, тәуекелдің мүмкін деңгейлерін негіздеу және талап ететін деңгейінің шараларын жоспарлау.

- Қауіпсіздік жүйесіне қажетті салымдарға экономикалық негіздеу, есептеу және потенциалды зияны мен шығынның арақатынасын белгілеу.

- Осалды қорларда пайда болатын шабуылдардың жүзеге асуына дейін бірінші кезектегі қауіпсіздік шараларын өткізу керек.

- Компанияның функционалды қарым-қатынасы, жауапты аймақтары мен жауапты адамдарды анықтау, ұйымдық-басқарушылық құжаттарды жасау немесе модификациялау.

- Бақылаушы және жауапты ұйымдармен келісе отырып, заман талабына сай ақпараттық технологияны өңдеу және дамыту.

- Ұйым жұмыстарының өзгеру шарттарына байланысты, ұйымдық-басқарушылық құжаттардың жүйелі өзгеруіне байланысты, технология-

лық процестердің модификациясы мен модернизациясына байланысты ақпараттық құралдарды жаңарту.

5.2 BS 7799 мен аудит қауіпсіздігі

5.2.1 Сараптау және аудит: ұйымдастыру аспектісі

Бүгінгі уақытта ең көп тараған ISO/IEC 27001:2005 (BS 7799-1:2000) "Ақпараттық технология – ақпараттық басқарудың қауіпсіздігі" (Information technology - Information security management) халықаралық сараптама. Бұл ақпарат Британдық сараптама BS 7799-1 "Ақпараттық қауіпсіздікті басқару мен практикалық кеңесінің 1-бөлімі бойынша жасалған" (Information security management, Part 1: Code of practice for information security management), бұл BS 7799-2:2002 сараптамасының екінші бөлімі тексеріс қауіпсіздігіне жатпайды. Сондықтан ақпараттық жүйені ISO/IEC 27001:2005 (BS 7799-1:2000) талаптарына сай деп айтуға болады. Бірақ ақпараттық жүйе сараптамасын BS 7799-2:2002 (Part II) орындауға болады. Тәуелсіз аудиттің бірігуі бойынша 7799-1 ақпарат жүйесі сараптаалады. Сараптама мәселелерімен Ұлыбританияда Британдық сараптама институты шұғылданады, (British Standards Institution - BSI) (www.bsi-global.com) оның бақылауында UKAS (United Kingdom Accredited Service) ұйымы аккредитация мәселесімен айналысады. Осы аталған ұжымдардың берген сараптамалары Ұлыбританияда ғана емес, дүние жүзінде танымал.

Ұжым, АҚ тексерісін жүргізгісі келсе, осы сараптамаға лайықты ақпараттық жүйе құжаттарын ретке келтіру керек. Тек қана содан кейін тексеруші шақырады. Тексеріс жүргізу тәсілдері төмендегідей.

Үлкен ұжымның жұмыс күні 25-30 тексеріс болып табылады.

Тексеріс өтіп болғаннан кейін сараптама АҚ BS 7799 сараптамасы бойынша беріледі, оның мерзімі – 3 жыл.

Ақпараттық жүйе қауіпсіздігінің және АҚ дамуын сұрақтарымен халықаралық Joint Technical Committee ISO/IEC JTC 1) және BSI институты, UKAS бөлімі шұғылданады. Бұл қызмет АҚ сараптамасын BS 7799-1 мен аккредитациялайды.

Ақпараттық жүйе сараптамасының тексеру процесін талқылаймыз.

5.2.2 Сараптама жүргізуге арналған әдістеме

Қолданылып жүрген амалдар мен Guide to BS 7799 risk assessment and risk management, Guide to BS 7799 auditing берілген бағалар бойынша сараптамаларды қарастырамыз. Бұл кеңестер отандық жағдайдағы ақпарат жүйесінде және кеңейтілген түрде қолдануға болады. Мұның ішінде тәуекелдікті бағалау соншалықты қымбат және қиын жобаны тілемейді.

Әрбір ұйым ақпараттық қауіпсіздік тексерісін өткізерде ұжымның құжаттарын, әдістемелерін алдын ала тексеріп, сараптама талабына сай дайындайды.

АҚ ұжымының тексерісі үлкен мұқияттылықпен талданады. Тексеріс жүргізушіге ұжымның тексеру жобасын ұсынады. Ең маңыздысы, тексеру сол ұжымның құқықтық-заңымен қай сараптамаға жататынын білу керек. Әрі қарай ұжымның нормативтік-әдістемелік құжаттарын тексереді. Тексеріске ұсынылған құжаттар: қауіпсіздік саясаты, қорғаныш жүйесінің шекарасы (корпоративтік жүйенің картасы, құрылымы, ақпарат жобасымен қамтамасыз етуі), корпоратив қызметкерлерінің қызметі жөніндегі нұсқаулар, ақпарат қауіпсіздігінің ережесі. Баға беру әдістемелері және оны пайдалану туралы кеңестері, ақпараттық жүйенің қауіпсіздігінің бағасы.

Бұған дейін тексеріс өткен болса, олардың жүргізген тексерісінің жазылған есеп баяндамасымен және ескертулермен танысу керек. Мұнымен қатар сараптамаға сәйкестендірілген ведомость болу керек.

АҚ жүйесінің ең маңызды сараптамасы – тексерістің барлық ережелерді орындауында. Тексеруші осы ережеге сәйкес барлық ереже сақталады ма, сақталмаса не себеп, соған жауап беруі керек. Сараптамаға сәйкес жұмыс жасалмаса ведомость толтырып, оның себебін түсіндіреді. Тексеріс жұмысы аяқталғанда, сәйкес келмеген ақпарат қауіпсіздігін жою мүмкіндігін туғызу керек. Тексеруші маман осы ұжымның BS 7799 сараптамасына сәйкес жұмыс жасап жүргендерін анықтап беру керек. Мұның бәрі құжаттармен расталып, анализ жасалынып, эксперттер кеңесінен кейін және қауіпсіздік режимі қажет жағдайда корпоративтік жүйесімен тексеруден өтеді.

Ең соңында ұйымның ақпараттық қауіпсіздігі, қызметкерлердің АҚның құжаттар саясаты және стратегиясы түгел түсіруден өткізілуі керек. Осыған байланысты құжаттардың стратегиялық және ережеге сәйкес қолданылуы мен бағалануы тиіс. Ұжымның дұрыс жұмыс жасап жатқаны қолданылып жүрген құжаттардың тәуекелділікке баруы қауіпсіздіктің режим журналы болып табылады.

Тексеруші ұжымының ақпараттық жүйесінің әкімшілік басқаруын, тәуекел бағасымен оның жиі тексерістен өткізуге рұқсатын, реестрін біліп отыруы керек.

Маман АҚ кезінде болған қорытындыны жасап отыру керек. Әрбір кездесіп отырған тәуекелді бағалап, құжаттармен дәлелдеп, келесі кезекте әрі қарай жұмыс бабына қолдану керек.

BS ISO/IEC кеңесін таңдап, ақпараттық жүйенің қауіпсіздігін, оның дұрыс қолдануын ұжым қызметкерлері АҚ саясатын тестілеу арқылы білулері тиіс. Тексеруші маман жұмыс аяқталған соң қорытынды жазу керек.

5.2.3 Тексеру қауіпсіздігінің тәсілдері

Тексерудің екі тәсілі бар болуы мүмкін: ұжым тексерісі және ақпарат жүйесінің тексерісі. Бірінші тәсілде:

- құжат, АҚ ұжымының қолданып жүрген бекітілген құжаттары, тәуекелдік бағамен жүргізілген құжаттар болуы;
- инфрақұрылымның қауіпсіздігі жазылған құжат – қызметкерлердің АҚ туралы міндеттері;
- қаралған жүйенің қорғау, қорғаушылық негізін таңдау;
- ақпарат жүйесінің әкімшілік басқару құжаты;
- тәуекел бағасы мен тексеру құжаты;
- қорытындылаған АҚ құжаты, оны орындау, тексеру және сақтықпен жұмыс жасау;
- АҚ құжатнамасы және жетекшілік тізімі (реестр), сәйкестендіру ақпарат тізімі болуы керек;
- ақпараттық жүйенің тәуекел бағалау қорытындысы болу керек;
- қолданылатын шаралар туралы құжат.

Осы айтылған тексерулер қорытындысы ұйымның тәуекелдік бағалау жұмысы мен жетекшілік жұмысы арқылы жүзеге асады.

АҚ ұжымында ақпарат жүйесі тексерісі болса:

- ақпарат қауіпсіздік саясатын басқару құжатын бағалау жүйесінің жай-күйін көрсететін құжат;
- тәуекел бағасының құжаты;
- АҚ орталығының құжаты;
- контрмер қолданғандағы қорытынды мен тест құжаты.

Бұдан басқа ақпарат жүйесін тексеруші міндетті түрде тексеріс кезіндегі туындаған сұрақтардың дұрыс-бұрыстығын білуі керек және сақтықпен тәуекел бағасын сараптау әдісін тексеру керек. Тексеріс кезінде кездесетін тәуекел бағасы сәйкес келе ме, дұрыстығын құжаттар бойынша мәліметтеу керек. Осының бәрін тексере келіп, АҚ-ке көз жеткізген соң, ақпараттық қауіпсіздік дұрыс, қызметкерлер, қауіпсіздік саясатымен таныс, құжаттар барлық сараптамаға сәйкес екеніне көз жеткізу керек. Қорытындылай келіп, сараптамаға сәйкес құжат әзірлейді.

Ең соңында ақпараттық жүйе және оның бөлімдерінде АҚ BS 7799 сараптамасы бойынша рұқсат беріледі, ол сараптама құжаты 3 жыл мерзімге дейін жарамды болады. Тексеріс кезінде тексеруші сараптамаға сәйкес анализ жасайды. Осы ұжымның маңызды аспектісі ақпарат қауіпсіздігінің қаншалықты қорғалуына, спецификасына және құндылығына анализ жасайды. Мұндай қорытындылау тексерушінің үлкен тәжірибелігін, білімділігін қажет етеді. Тексерушінің қорытындысы бойынша кеткен кемшіліктер мен ескерту тізімі сараптамаға сәйкес жасалады. Тексерушілер осы процестерді түзету үшін күш салу керек. Осыған орай тексеруші мен ұйым осы кемшіліктердің қаншалықты қиын және оны қалай түзету жо-

лын қарастырады, сараптамада сәйкес келмеушіліктің келесі санаттары қарастырылған. Басты сәйкес келмеушілік: сараптаманың сақтық түрі жасалмаған немесе ұйымның маңызды ақпаратына түрлі әдіс қолданылған. Жай сәйкес келмеушілік: ақпарат қауіпсіздігі әртүрлі себеппен қорғалмаған, ақпарат тәуелділігінің қорғау қабілетін азайтқан.

Сәйкес келмеушілікте BS 7799 сараптамасына сүйеніп жұмыс жасайды. Осындай сәйкес келмеушілік көбейіп бара жатса, тексеруші оны алдын ала зерттеу керек. Оны ұйым мен тексеруші бірігіп, зерттеулер жасап отыру керек. Ақпараттық жүйенің бөлімдерінде тексеруші жаңалықтар қосып отырса, оны құжаттарға тізіп отырады. Ұжымның тексерушіге қарымқатынасы әртүрлі болуы мүмкін. Өйткені әр ұжым оны қалай түзету керек екенін өздері шешеді.

Ескертулер келесі тексеріс кезінде керек болады. Кеткен кемшіліктерді тексеруші түзетілгенін, не болмаса орындалмай жатқанын білу керек. Тексеруші бұрынғы құжаттарға анализ жасайды. Қайта жасалған тексеру кезіндегі құжатқа сәйкестендіру ведомосі жасалады.

5.2.4 Тексеру өткізу

Тексеру жұмысын ресми кіріспе жиналыспен ашады. Жиналыста АҚ қызметкерлерге, жетекшілерге, орта және жоғары буынға ескереді:

- тексеру жұмысының жобасы, қашан және қай уақытта;
- тексеру кезінде қолданылатын бағалау әдістемесі;
- сәйкес келмеушілік және оны жою;
- тексеру кезіндегі ескертулер және оның себептері;
- жетекшілікке алатын құжат және оған жұмыс істеу ережесі;
- тексеру кезіндегі қиындықтар;
- сәйкес келмеушілік, ережелер, айтуға болмайтын ақпараттар туралы түсініктеме.

Ұйымның әкімшілігі тексеру кезінде ақпараттық жүйенің осал жерлеріне көбірек көңіл аударылатынына дайын болу керек: пароль тізімі корпоративтік есепке алу, жеке іс қағаздары. Тексеру аяқталған соң қорытынды жиналыс өткізіледі және мәселе қойылады:

- тексеруге берілген жұмыс көлемі мен шегі, оның қалай болғаны;
- қысқа мазмұны сәйкес келмеушілік және өзгертулер;
- ескертулер мен жаңарту тәсілдерімен танысу;
- тексерістің қалай жүргені және оны баяндау;
- қорытындыдан немесе сараптамадан бас тарту. Егер болмаса әрі қарай жұмыс істеу;
- алған міндеттемелердің жасырын сақталуы.

Қорытынды жиналысқа қатысушылар ресми түрде тіркелуі тиіс. Тексерушінің басты қорытындысы ресми баяндау болып табылады:

- BS 7799, ақпараттық жүйедегі сараптама деңгейі осы сараптамаға сай келуі керек. АҚ қауіпсіздігінің тексерісіне жүргізілген жоба бойынша сәйкес келуі, ведомостік сәйкес келуі;

- ұйымның жұмыс жүргізіп отырған саясат қауіпсіздігі, ведомостік сәйкестігі, процедураның сай келуі, қосымша міндеттері, нормалары кеңінен айтылуы керек;

- жалпы ескертулер;

- сандық және санаттық көрсеткіштері;

- қосымша тәсілдердің керек екенін негіздеу және оның жалпы жобасы;

- тестке қатысушы қызметкерлердің тізімі.

Бұл есеп беру тексерудің ресми құжаты, есеп берудің түпнұсқасы сараптама ұйымына беріледі. BS (ISO/ IEC) сараптамаларына сәйкес тексеру ұйымының аспектілік АҚ анықтап тұруы керек.

Есеп беру, тексеру өткен сайын жаңарып отырады. BS 7799 АҚ сараптамаларын, АҚ сараптама беретін ISO 9001 және ISO 9002 рұқсат етеді. Бітірілген сараптама алу үшін BS 7799 сараптама шарттары қолданылады.

Біріккен тесттен өту үшін АҚ процедурасын өткізу керек, сараптама беру үшін тексеру ұжымы кепілдеме береді.

5.3 Ақпарат жүйесінің тексерісі: COBIT 3rd Edition кеңестері

Қазіргі уақытта тексеруші компаниялар мемлекеттік және мемлекеттік емес ассоциацияға біріккен, олардың құрамында кәсіпқой білімгерлер бар. Олар ақпараттық технологияда стандарттарды сақтықпен қорғай отырып құрады.

5.1-кесте

Ақпараттық технологияның сараптамаларын салыстыру

	COBIT	**SAC**	**COSO**	**SAS 55/78**
Аудит мақсаты	ТОР менеджер, қолданушылар, АЖ тексерушілері	Ішкі тексерушілер	ТОР-менеджерлер	Сыртқы тексерушілер
Аудит түсініктемесі	Саясат қауіпсіздігін өңдеудің эксплуатациялық нормасы	Бизнес процесті жүйелі түрде тексеру. Саясат қауіпсіздігі және кадр саясаты	Бизнес процесті жүйелі түрде тексеру. Саясат қауіпсіздігі және кадр саясаты	Бизнес процесті жүйелі түрде тексеру. Саясат қауіпсіздігі және кадр саясаты
Тексеру мақсаты	Бизнесті дамыту, оның маңызын арттыру, нормативтік-құқықтық базасын ұстану	Бизнесті дамыту, оның маңызын арттыру, нормативтік-құқықтық базасын ұстану	Бизнесті дамыту, оның маңызын арттыру, нормативтік-құқықтық базасын ұстану	Бизнесті дамыту, оның маңызын арттыру, нормативтік-құқықтық базасын ұстану

Қолдану	Жоспар және ұйымдастыру, мақсат қою, оны орындау мониторингі	Өндірісті дамыту, автоматизацияланған жүйені жүргізу	Өндірісті дамыту, тәуекел-менеджмент, АЖ басқару, корпорациялық және АЖ-ның мониторингі	Өндірісті дамыту, тәуекел-менеджмент, АЖ басқару, корпорациялық және АЖ – ның мониторингі
Акцент	Ақпараттық технологияның менеджменті	Ақпараттық технологияның менеджменті	Менеджмент	Қаржылық менеджмент
Тексеруші сертификатының мерзімі	Уақыт интервалы	Тексеріс уақыты	Уақыт интервалы	Уақыт интервалы
Естіген тұлғалар	Ұжымның TOP-менеджерлері	Ұжымның TOP-менеджерлері	Ұжымның TOP-менеджерлері	Ұжымның TOP-менеджерлері
Тексерісті жүргізетін құжаттардың көлемі	187 беттен тұратын 4 құжат	1193 беттен тұратын 12 бөлім	353 беттен тұратын 4 том	63 беттен тұратын 2 құжат

Тексерушілер ассоциациясының (Information Systems Audit and Control Association-ISACA) басқа ұйымдардан айырмашылығы, ақпарат жүйесінде ашық тексеріс жүргізеді. Ассоциация 1960 жылы ашылған. Оның қатарында 100 елден астам, 23000 адам құрайтын мүшелері бар, Қазақстанда да мүшелері бар.

ISACA ассоциациясы бір жерде шоғырланған, 26000-нан астам тексерушісі бар. (CISA-Certified Information System Auditor) Өздерінің сараптама жүйелері бар, зерттеулер жүргізеді және кадрлар даярлайды, конференциялар өткізіп тұрады.

ISACA ассоциациясы ақпарат жүйесінде АҚ мәліметтерін жинақтайды, ұйымның қауіпсіздік ресурсын қамтамасыз етеді, маңызды ақпараттық технологияның мақсаты орындалуын бақылайды. ISACA-ның негізгі мақсаты – зерттеу, өңдеу, құжаттардың сарапталған ақпарат жүйесіндегі дамуы және оның күнделікті қолдану тәсілдері.

Ассоциация өзінің ақпараттық технологиялық концепциясын АҚ жүйесінің талабына сәйкестендіріп отырады. Осы концепция бойынша ақпараттың технология элементі арқылы жетекшілік жүйесіне және АҚ режиміне кепілдеме береді. Бұл компания COBIT 3rd Edition-Control Objectives for Information and related Technology (ақпарат технологиясының қабылдаушысы), ол 4 бөлімнен тұрады:

1-бөлім: концепцияның қысқа түрі (Executive Summary).

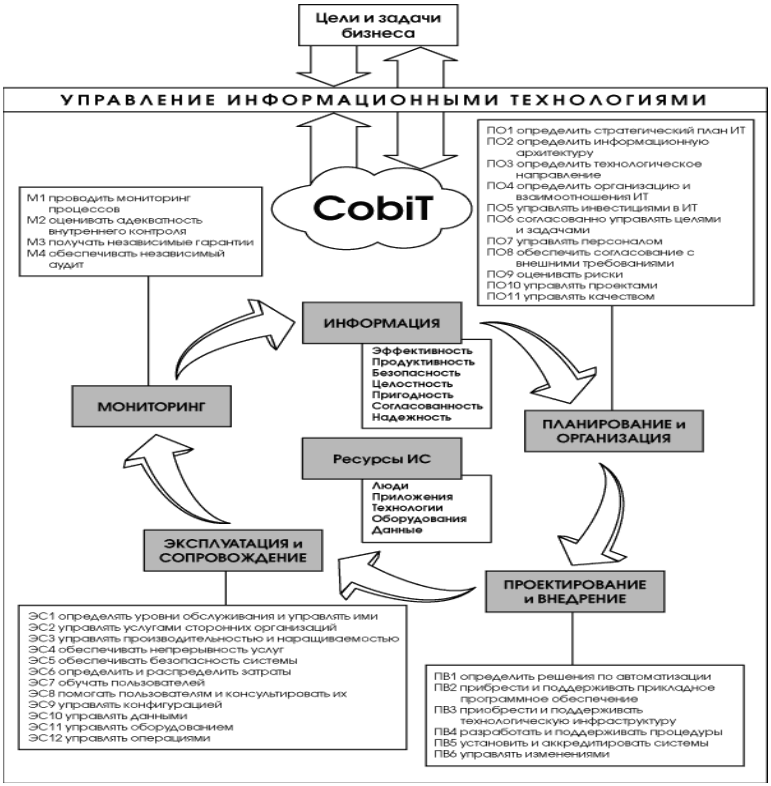
2-бөлім: негізгі түсініктері мен анықтамалары (Framework). Бұдан басқа талаптары да жазылған.

3-бөлім: мүмкіндік инструментарийі және жетекшілік процесінің ерекшелігі (Control Objectives).

4-бөлім: компьютерлік ақпарат жүйесіндегі кепілдемелердің орындалуы (Audit Guidelines).

Бұл құжаттың 3 бөлімі халықаралық стандарт BS ISO/IEC 7799 (BS 7799) сияқты. Бұл АҚ практикалық кеңестері мен оның жетекшілігі туралы кеңінен жазылған. Бірақ модельдік жүйесінде айырмашылық бар. COBIT стандартының құжаттары ашық түрде болады. Ол 1996 жылы бірінші рет жарыққа шықты. Ол ақпараттық технологияның моделін 5.1-суретте кең түрде суреттеген.

Ең негізгі мақсаты: ұйымның қажетті және керекті ақпараттарын жинақтап біріктіру. COBIT моделінде ақпарат технологисының қорлары бар, олар ақпарат көзі болып табылады. Ақпарат технологиясы бизнес-процестің талабына сай болуы керек. Бұл талаптар мына түрде шығарылған.



5.1-сурет. Ақпараттық технологияны басқару моделі

Біріншіден, ақпараттың маңызды өңделуі және оның суреттемесі талапқа сай өңделген ақпарат оның көлеңкелі аспектісін баяндайды, керек

жерінде қолданады. Бұл топқа мынадай көрсеткішті қосуға болады. Ақпараттың субъективті аспектісінің интерфейсті ыңғайлы стилі.

Екіншіден, технологиялық сенім – бұл көрсеткіш ақпарат жүйесінің сараптамаға сай келуі. Сенімділігі, жұмыс істеу амалдары.

Үшіншіден, АҚ көрсеткіштері – жасырын түрдегі (таратуға болмайтын) хабарлар және олардың бірегей қолданылуы.

5.3.1 Сараптама жүргізу этаптары

Тексеру кезеңінің шартын жасағанда ұйымның атынан және тексеруші ұйымынан рұқсатнама құжаттарына екі жақтан қол қойылады. Тексеру өткізіледі, бақылау элементтері туралы құжат жасалынады. Алдын ала ақпарат жүйесіндегі ақаулы жерлер терең зерттеледі.

Зерттелген жүйе COBIT сараптамасына сүйене отырып, оның бақылау жүйесі мен ақпарат жинау кезеңін бастайды. Бақылауда ақпараттық жүйе бақылайтын элементтерін көрсетеді. Осы арқылы зерттеу мақсатының құндылығына, шығынына, үйлесімді арақатынасына жетуге талпынады. Бастапқы ұсынудың бинарлық жауабы ИӘ/ЖОҚ деп өзгереді. ISACA ассоциациясы бірқатар талаптар қойды, ол COBIT сараптамасында іске асты.

Ақпаратқа қойылатын талап түсінікті, пайдалы, мамандар үшін қажет болу керек. Ақпарат орынды болу үшін қолданушыларға өткен, болып жүрген, алдағы уақытта хабарларды ыңғайлы шешіп, кеткен қателерді түзету үшін керек.

Кей кезде ақпараттық тексеріс кезіндегі кеткен қателіктер түзеліп отырса, өндірістің дамуына бөгет болмайды. Сенімдірек болу үшін шын бейнетораптық қол жеткізетін ақпарат болуы керек.

Анализдеу кезінде бастапқы хабарда ескеріледі. Бастапқы хабарға қойылатын талап хабар жинақтау кезінде қолданылады. COBIT стандарты өзінің кеңестері мен әдістемелерін ұсынады және ISACA рұқсатымен басқа да өңдеулерді жетілдіруге болады. Анализдеу кезінде ақпарат жиынтығының жетіспеген ақпаратын бастапқы хабардан алуға болады.

Келесі кезең – кепілдемені өңдеу. Анализден кейін ұйымның жетекшілерімен келісе отырып, өзекті және қаншалықты тәуекелді өтетін жағдайын білу. COBIT стандарты ақпараттық жүйенің жағдайы туралы кепілдемені есеп беру арқылы жасатады. Тексеру қорытындысын 3 топқа бөлуге болады: ұйымдастырушылық, техникалық және методистік. Бұл 3 топтың әрқайсысы ұйымдастырушылық, техникалық және методистік ақпарат жүйесін қамтиды.

Ұйымдастырушылық бөліміне: стратегиялық жоба, жалпы жетекшілік ақпарат жүйесі инвестициясы, кепілдемесі, ұйымның бәсекелестігі, ақпарат жүйесінің аз мөлшерде шығыны, шығынды аз жұмсауға арналған әртүрлі тәсілдер, тәуекелділік, ақпараттық жүйенің бір жолғы жобасы.

Техникалық бөлім ақпараттық жүйенің керекті жағдайын, аз мөлшерде шығын шығарудың амалын қарастыру, техникалық шешімді бағалау, кәсіби тұрғыдан функционалды жағдай және керек болғанда модернизациялау, шын жұмыс істеу деңгейін белгілеу болып табылады.

Методологиялық қорытынды: стратегиялық жоба және болжамдау, құжат айналымын оптимизациялау, еңбек тәртібін күшейту, оқыту, дер кезінде ақпарат жүйесі жөнінде хабар алу. Бақылауды тексеруші фирма жүргізіп, зерттеп отырады.

Бұдан кейін есеп беру аспектісінің ақпараты бойынша тексеріс графигі, кеңейтілген және қысқартылған жоба, төтенше жағдай кезіндегі өз қалпына келтіру жобасы, зиянкестік болғанда қорғауды жүргізу тәсілдері.

Жиі жүргізілген тексеріс жүйенің дұрыс жұмыс атқаруын арттырады, сондықтан кәсіби тексерушінің жасаған графиктері басты шарт болып есептеледі.

COBIT моделіндегі ақпараттық технология өмір циклінен өтеді:

Ұйымдастырушы және жобалау. Бұл стадияда стратегиялық және тактикалық ақпарат технологиясы бизнестің негізгі мақсаты болып табылады, сосын әрі қарай дамыту сұрақтары туындайды: жүйенің архитектурасын, технологиясын, қаражатпен қамтуын және т.б. Бұл стадияда алға қойған 11 негіз бар.

Амалдау және жинақтау. Бұл кезде шешім құжатталған және жоспарланған түрде болу керек. Осыған байланысты 6 шешім бар.

Қолдау және қолдану. 13 негізгі шешім кезеңі бар. Бұл ақпарат технологиясын жүргізуге арналған.

Мониторинг. Ақпарат технологиясының параметрлерін бақылау. 4 негізгі шешімі бар.

COBIT сараптамасында 34 жоғарғы деңгейдегі шешімі бар. Үйреншікті ақпараттан (жасырын, қол жетерлік, бүтіндік) басқа 4 негізгі шешімі бар. Олар: әрекеттілік, нәтижелік, сәйкестік және сенімділік. Бастапқы үшеуі бір-бірімен тәуелді.

Егер ақпарат жүйесінің жобасы мен өңдеуі оларды комплектілеу және жүзеге асыру, мониторингтеу, қолдану болса COBIT сараптамасы ұсынылады. Сараптама 4 базалық топтан 34 бөлімшеден, оның өздері 318 бақылаушыдан тұрады. Олардың әрқайсысы сараптамашыларға жеткілікті ақпараттар беріп отырады.

АҚ жүйесіндегі жинақтар жетекші құжаттарды береді. Сараптама құжаты заман талабына сай концептуальды амалдарды зерттеп, кепілдеме түрінде дамытуға жинап береді.

COBIT сараптамасы ISA ISACF базасында болады және халықаралық сараптамада нормативтік құжат, техникалық стандарт, кодекс, ақпарат жүйесін бағалау, кәсіби стандарт, банк жүйесі, электрондық сауда, өндірісті сипаттайды. Сараптама консалтингтік ұйыммен жобаланған және

сонымен жұмыс жасайды. Аз мөлшерде болса да, сараптама өндірістік ұйымдардан тәуелсіз.

Сараптаманы жобалаған кезде оның жұмыс істей алатын мүмкіндіктері қарастырылған, оны жобаға және тексеру жұмысына қолдануға болады.

Бірінші жағдайда, зерттелген жүйенің деңгейін анықтай алады. Екіншіден, сипаттамасы бойынша ең биік дәрежедегі жүйені жобалайды.

COBIT сараптамасы ұқсас жобалардан ұтымдылығымен ерекшеленеді. Сараптаманың ерекшеліктері оның жеткілікті, оңай шешімді, ақпарат жүйесінің кең көлемде және кеңейтіліп қолданылуында. Ақпарат жобалық шешімді өзінің құрылымын өзгертусіз қолдана беруіне болады. Сараптама сипаты оның үлкен шешімді диапазонында – стратегиялық жобадан бастап, кішкентай бөлшектерді сұрыптай алатындығында және ақпарат жүйесінің осал жерлері мен сын көтермейтін жерлерін бақылайды.

ISACA ассоциациясы тексерушінің регламентімен әртүрлі аспектілік жұмысына үлкен көңіл бөледі. Тексерушінің кәсібишілігі және регламенті біріксе, ақпарат жүйесіндегі мықты маман болуын қамтамасыз етеді. Тексерушінің негізгі құжаты регламенттік мандат болып табылады.

Қолында CISA сұрыптамасы бар тексеруші мандатында мынадай ақпарат болу керек:

- Тексерушінің міндеті мен жауапкершілігі (Responsibility), тексеру көрсеткіштері, маңызды факторлары, тексерушінің ең керекті деген талаптары, тәуелсіз тексерушінің гарантиясы, тексеру ауқымы. Осыларды жүргізу үшін ресми рұқсаты болуы керек.

- Тексерушінің үстемдігі (Authority), компьютерлік ақпарат жүйесінің бөлігі, тексеру жүргізу құқығы жүргізілетін шаралардың осындай тәуекел жиынтығы.

- Тексерушінің есеп беру міндеті (Accountability) ақпараттың ережесін, тәуелсіз бағалау процедурасын, негізгі қорытындыларды ұйымның жетекшілеріне реттеп береді.

Қазіргі заманның ақпараттық қауіпсіздік жетекшілігі қандай сұрақ болса да шешімін табады. Технологияның қауіпсіздік деңгейі өте жоғары деңгейде болады. Бірақ өте жоғары деңгейдегі қауіпсіздікті қолдануға шығын көп кетеді. Сондықтан қатты шығынға батпай, өз деңгейінде оңтайлы жағдайды таңдай білуі керек. Кішкене бөлімдердегі көрсеткіштер оның қаншалықты тиімді екенін және өлшемдерін, тәуелділік деңгейін, мониторинг жүйесінің қадағалап отыру бағытын ұстанады. Мұндай шешімді қабылдау өте күрделі.

АҚ дұрыс қабылдап бағалау, контрмер жүйесін таңдау, маңызды баға қатынасын білу – тексерушінің ең керектісі.

ISACA оқу жобасы бар, ол осындай керекті білгірлікке көмектеседі. TAKO атты интерактивті оқыту жобасын қарастырамыз: http://www.isaca.org/tako.htm.

VI ТАРАУ

АҚПАРАТТЫҚ ЖҮЙЕНІҢ ҚАУІПСІЗДІГІН ТАЛДАУ

Қазіргі таңда автоматтандырылған жүйенің (АЖ) қауіпсіздігін талдайтын белгілі бір стандартталған әдісі жоқ, сондықтан нақтылы жағдайларда аудиторлардың іс-әрекет алгоритмі әртүрлі болуы мүмкін. Алайда бірлескен желінің қауіпсіздігін талдайтын типтік әдісті ұсынуға болады. Бұл әдістің тиімділігі талай мәрте тәжірибеден тексерілген.

Типтік әдіс келесі тәсілдерден тұрады:

– АЖ бойынша бастапқы мәліметтерді зерттеу;

– АЖ қауіпсіздігінің қауіп-қатеріне байланысты қорларының тәуекелділігін бағалау;

– Ұйымдастыру деңгейінің қауіпсіздік механизмін, ұйымның қауіпсіздік саясатын және ақпараттық қауіпсіздік тәртібін қамтамасыздандыру бойынша ұйымдастыру – басқару құжаттамасын талдау, олардың бар нормативті құжаттамалардың талаптарына сәйкестігін және де олардың болатын тәуекелдерге теңбе-тең келетінін бағалау;

– Бағыттауыштардың конфигурациялы файлдарын, желіаралық экран (ЖЭ) және желіаралық өзара әрекеттерін, пошталық және DNS-серверлерді, сонымен қатар басқа да желілік инфрақұрылымның сыни элементтерін басқаратын proxy-серверлерін талдау;

– Internet желісінен жергілікті есептеуіш желісінің (ЖЕЖ) ішкі желілік адресін сканерлеу;

– (ЖЕЖ)-нің қорларын іштей сканерлеу;

– (ЖЕЖ) серверлерінің сырт пішінін және жұмысшы станцияларын арнайы бағдарламалық амалдар көмегімен талдау;

Зерттеудің аталған тәсілдері қорғау жүйесінің активті және пассивті тестілеуін алдын ала қарастырады. Қорғау жүйесінің активті тестілеуі қорғаудың механизмдерін жеңу үшін потенциалды қаскүнемнің әрекеттерін эмуляциялау болып табылады. Пассивті тестілеу ОЖ сырт пішінін және тексерістің тізімін қатыстыратын шаблон бойынша қосымшасының талдауын көздейді. Тестілеуді қолмен атқаруға немесе арнайы бағдарламалық амалдар арқылы жүзеге асыруға болады.

6.1 Бастапқы мәліметтер

Келісілген міндеттемелерге сәйкес, алдын ала тексерісті және информатизациялау объектісінің қорғаныс талдауын қамтитын АЖ қауіпсіздігінің аттестациялау жұмысын жүргізу барысында тапсырушы келесі бастапқы мәліметтерді беру қажет:

– информатизациялау объектісінің толық және дәл атауы мен оның тағайындалуы;

– ақпараттың сипаты (ғылыми-техникалық, экономикалық, өндірістік, қаржылық, әскери, саясаттық) және оның қандай тізімге (мемлекеттік, салалық, мәліметтік, кәсіпорындық) сәйкес анықталғанының жасырын деңгейі (құпиялылығы);

– информатизациялау объектісінің ұйымдастырылу құрылымы;

– ғимараттар тізімі, көрсетілген ақпарат өңделетін информатизациялау объектісіне енетін техникалық амалдар (негізгі және қосымша) жиынтығының құрамы;

– информатизациялау объектісінің бақыланатын аймағының шекараларының көрсетілуімен орналасқан схемасы және ерекшеліктері;

– тексерілетін объектіде орнатылған және ақпаратпен алмасу хаттамасымен кабылданған қорғалатын ақпаратты өңдеу үшін арналған бағдарламалық қамтамасыздандыру құрылымы (жалпыжүйелік және қолданбалы);

– ақпараттық ағымдар және қорғалатын ақпараттың өңдеу тәртібінің схемасымен қоса, информатизациялау объектісінің жалпы функционалды схемасы;

– басқа информатизациялау объектілерімен өзара әрекеттесу сипаты және бар болуы;

– тексерілетін объектідегі ақпараттың қорғау жүйесінің құрамы және құрылымы;

– қорғалған атқарудың техникалық және бағдарламалық амалдарының тізімі, тексерілетін объектіге енгізілген қорғаудың және бақылаудың амалдары және ие болатын сәйкес сертификат, яғни пайдалануға берілген ұйғарым;

– ақпаратты қорғау жүйесінің өңдеушілері туралы мәлімет, жақтаушы (тексерілетін объект орналасқан өнеркәсіпке қатысты) өңдеушілердің сол тәрізді жұмыс өткізуіне лицензиясының бар болуы;

– объектіде (бұл объект орналасқан өнеркәсіп) ақпарат қауіпсіздігі қызметінің, администратор қызметінің (автоматтандырылған жүйесі, желісі, мәліметтер қоры) қатысуы;

– информатизациялау (қорғалатын ақпарат өңделетін және ақпараттық таратушылары сақталатын ғимарат) объектінің физикалық қорғауының негізгі сипаттамалары және қолданылуы;

– жобалық және пайдалану құжаттамаларының және де тексерілетін объект бойынша ақпараттың қауіпсіздігін анықтайтын басқа бастапқы мәліметтердің дайындығы,сонымен қатар бар болуы.

Тәжірибе бойынша аталған бастапқы мәліметтер АЖ қорғауының талдауы үшін жеткіліксіз. Бұл тізімнің соңғы пунктінде информатизациялау объектісі бойынша ақпараттың қауіпсіздігіне әсер ететін басқа бастапқы мәліметтер берілуі болжанады. Дәл осы «қосымша» мәліметтер ағымдағы АЖ қауіпсіздігінің қамтамасыздануының жұмыс жағдайын бағалау үшін өте маңызды болып табылады. Төменде сәйкес құжаттар аталған.

Қосымша құжаттама:

– регламентті жұмыстарды атқару бойынша нормативті-басқарушы құжаттар;

– қауіпсіздік саясатын қамтамасыздандыру бойынша нормативті-басқарушы құжаттар;

– администраторлар, техникалық қолдаудың инженерлері және қауіпсіздік қызметінің лауазымды нұсқауы;

– ақпараттық қорларға және олар реттеуіне НБЖ әрекеттерін болдырмау жоспары және процедуралары;

– IP-адресінің көрсетілуімен бірлескен желінің топология схемасы және құрылымдық схемасы;

– әрбір қордың құпиялылығы мен сыншыл деңгейі көрсетілген ақпараттық қорлардың құрылымы бойынша мәліметтер;

– бірлескен желідегі ақпараттық қорлардың орналасуы;

– қолданушылардың ұйымдастыру құрылымының схемасы;

– қызмет көрсету бөлімшелердің ұйымдастыру құрылымының схемасы;

– мәліметтерді жіберу сызығының орналасу схемасы;

– АЖ объектісінің жерге қосылуының және электржабдықтамаларының жүйесінің сипаттамасы және схемасы;

– желілік басқару және мониторингтің пайдалану жүйелері туралы мәліметтер.

Жобалық құжаттама:

– функционалды схемалар;

– автоматтандырылған функциялардың бейнесі;

– негізгі техникалық шешімдердің бейнесі.

Эксплуатациялық құжаттама: қолданушылар және ақпаратты қорғау құралдарының (АҚҚ) бағдарламалық және техникалық амалдарын қолданатын администраторы үшін қажетінше басқару.

6.1.1 ЖЕЖ ішкі периметрінің қорғау амалдарын талдау

ЖЕЖ ішкі периметрінің қорғау амалдарының конфигурациясын талдау және желіаралық өзара әрекетті басқару кезінде конфигурация арқылы анықталған келесі аспектілерге зор көңіл бөлген жөн:

– ЖЭ-ға және бағыттауыштарға кіруді (желілік пакеттердің сүзгілеу ережелері) шектеу ережелерін реттеу;

– Аутенфикацияның параметрлерін реттеу және қабылданған схемалары;

– Оқиғаны тіркеу жүйесінің параметрлерін реттеу;

– Қорғалатын желі топологиясының жабылуын қамтамасыздандыратын және (NAT) желілік адресінің трансляциясын қамтитын механизмдерді қолдану және split DNS домендік аты бар қорғау жүйесі қызметін қатыстыру;

– Шабуыл және соған орай әрекет ететініні туралы хабарлайтын механизмін реттеу;

– Бүтіндікті бақылау амалдарының бар болуы және жұмысқа қабілеттігі;

– Орнатылған БЖ (ПО) нұсқасы және бағдарламалық түзету пакеттерінің бары.

6.2.1 Қорғау жүйесінің тестілеу әдістері

АЖ қорғау жүйесін тестілеу онда бар қорғау механизмдерінің тиімділігін мүмкін болатын шабуылдарға қарсы тұрақтылығын тексеру, сонымен қатар қорғау кезінде әлсіздігін іздеу мақсатында жүргізіледі. Дәстүрлі түрде тестілеудің екі әдісі қолданылады:

– «қара жәшік» әдісі;

– «ақ жәшік» әдісі.

«Қара жәшік» әдісі бойынша тестілеу, бұл тестілеуді өткізетін жақтың сынау объектісінің ішкі құрылымы мен конфигурация туралы арнайы білімі жоқ деп болжау. Мұндай тестілеу әдістері қорғау жүйесін бұзатын потенциалды қаскүнемнің әрекетіне зиян келтіреді. Тестілеудің негізгі амалы атақты әлсіздіктері бар мәліметтер қорында орналасқан желілік сканерлер болып табылады.

«Ақ жәшік» әдісі сынау объектісінің конфигурациясын және құрылымы туралы білім негізінде тестілеудің бағдарламасын құруын жүзеге асырады. Тестілеу барысында қауіпсіздік механизмінің бары және жұмысқа қабілеттігі, қорғау жүйесінің конфигурациясының және құрамының қауіпсіздік талаптарына және бар тәуекелділіктерге сәйкестігі тексеріледі. Әлсіздік туралы тұжырым жүйелік БЖ және қорғаудың енгізілген амалдарының конфигурациясын талдау негізінде жасалады, содан соң тәжірибеде тексеріледі. Талдаудың негізгі құралы – төменде қарастырылатын жүйелік деңгейдің қорғанысын талдау амалдарының бағдарламалық агенттері.

6.2 Қорғаныс талдауының амалдары

АЖ қорғанысы талданатын бағдарламалық амалдар өте көп. Көптеген жағдайларда кең таралған бағдарламалық өнімдер коммерциялықтардан кем емес. NESSUS коммерциялық емес сканерін оның коммерциялық аналогтарымен салыстырсақ жеткілікті.

ОЖ қорғанысын талдаудың өте ыңғайлы және қуатты амалы болып келесі бейнелетін, еркін таратылатын бағдарламалық өнім CIS Windows 2000 Level 1 Scoring Tool, сонымен қатар ОЖ өңдеушілері тегін ұсынатын осыған ұқсас амалдары Solaris ОЖ үшін ASET немесе Windows 2000 ОЖ үшін MBSA (Microsoft Security Baseline Analyzer).

Үлестірілген компьютерлік жүйелердің қорғанысының бақылауы мен талдау процестерін автоматтандырудың бір әдісі интеллектуалды бағдарламалық агенттердің технологиясын қолдану болып табылады. Қорғау жүйесі консоль/менеджер/агент архитектурасы бойынша құрылады. Бақыланатын жүйенің әрқайсысына БЖ реттеуіне сәйкес орындалатынын және олардың дұрыстығын тексеретін, файлдардың бүтіндігін, бағдарламалық түзету пакеттерін уақытылы орнатылуын бақылайтын, сонымен қатар АЖ қорғанысын бақылауының басқа да пайдалы есептерін орындайтын бағдарламалық агент орнатылады (желі бойынша агенттерді басқару менеджер бағдарламасы бойынша жүзеге асырылады). Менеджерлер мұндай жүйелердің орталық құрауышы болып табылады. Олар домен арқылы бақыланатын барлық агенттерге басқару командаларын жібереді де, агенттерден алынған барлық ақпаратты орталық мәліметтер қорында сақтайды. Администраторлар қауіпсіздік саясатын құруға, күйге келтіруге және таңдауға, жүйенің өзгеру жағдайын талдауға, әлсіздікті жоюға және т.б. мүмкіндік беретін графикалық консоль арқылы менеджерлерді басқарып отырады. Агенттер, менеджерлер және администраторлар арасындағы барлық өзара әрекеттер қорғалған клиент-серверлік хаттама арқылы іске асырылады. Мұндай тәсіл Symantec ESM ұйымының қауіпсіздікпен басқарудың комплексті жүйесін құру кезінде қолданылған.

Қорғаныста талдаудың тағы бір кең таралған түрі бұл - АЖ басып енетін, желілік әрекеттер жасайтын потенциалды қаскүнемнің әрекетіне зиян келтіретін қорғау механизмінің активті тестілеуі. Мұндай мақсат үшін потенциалды бұзақылардың әрекеттеріне зиян келтіретін желілік сканерлер қызмет етеді. Желілік сканердің жұмысының негізінде атақты әлсіздігі бар ОЖ, ЖЭ, бағыттауыштар және желілік сервистерден тұратын, сонымен қатар басып енетін (шабуыл сценарийі) әрекеттердің алгоритмін қамтитын мәліметтер қоры жатады. Қарастырылатын келесі Nessus және Symantec NetRecon желілік сканерлер қорғаныс талдауының бағдарламалық амалдарының берілген лайықты класын көрсетеді. Осылайша, бұл бағдарламалық амалдарды шартты екі класқа бөлуге болады. Бірінші класқа тиесілі желілік сканерлерді, кейде желілік деңгейдің қорғаныс талдауы-

ның амалы деп те атайды. Екінші класқа қалған желілік сканерлерді, кейде жүйелік деңгейдің қорғаныс талдауының амалы деп те атайды. Дәл осы амалдардың кластары өзінің артықшылықтары және кемшіліктері бар, алайда тәжірибеде олар бір-бірін толықтырады.

Желілік сканердің жұмыс істеуіне талданатын жүйелерге желілік кіру мүмкіндігі бар тек қана бір компьютер қажет, сондықтан бағдарламалық агенттердің технологиясында құрылған өнімге қарағанда, әрбір талданатын жүйеде өзіндік (әрбір ОЖ үшін) агентті орнату қажет емес.

Желілік сканердің кемшілігі бір жүйеден барлық желілік компьютерлерді сканерлеу үшін уақытша шығындар және желі құруына түсетін үлкен жүктеме қажет. Одан басқа, жалпы жағдайда сканерлеуден шын шабуыл әрекеттер сеансын ажырату қиынға соғады. Желілік сканерлерді қаскүнемдер де жиі қолданады.

Интеллектуалды бағдарламалық агенттерде құрылған қорғаныс талдауының жүйесі желілік сканерлерге қарағанда мықтырақ болып келеді. Алайда барлық артықшылықтарына қарамастан, бағдарламалық агенттер желілік сканерлерді алмастыра алмайды, сондықтан екеуін бірлесіп қолданған жөн. Сканерлер жай, қолайлы, арзан және көп жағдайда қорғаныс анализінің тиімді амалы болып табылады.

6.2.1 Security Benchmarks спецификациясы

Компьютерлік жүйелердің қауіпсіздік қауіп-қатерден қорғаныс деңгейі көптеген факторлардан тәуелді. Анықталатын факторлардың бірі қолданбалы және жүйелік БЖ конфигурациясының, ақпаратты қорғау амалы және бар тәуекелділіктерге активті желілік жабдықтың дәлме-дәлдігі. АЖ аталған компоненттердің жүздеген параметрлері бар, жүйенің қорғанысына әсерін тигізетін мәндері, яғни олардың талдауы қиын орындалатын есепке айналады. Сондықтан қазіргі АЖ қолданбалы және жүйелік БЖ конфигурациялы параметрлерінің талдауы, ақпараттың қорғау амалы және техникалық амалдары үшін арнайы бағдарламалық құралдар қолданылады.

Қорғау параметрлерінің талдауы қажетті қорғаныс деңгейін қамтамасыздандыру үшін міндетті түрде орнатылған параметрлердің тізімі және мәндерінен тұратын шаблондар арқылы жүзеге асырылады. Әртүрлі бағдарламалық-техникалық құралдар үшін әртүрлі шаблондар беріледі.

Internet желісіне қосылған коммерциялық бірлескен желі туралы қорғаныстың негізгі деңгейі жеткілікті деп айтуға болады. Қорғаныстың негізгі деңгейін қолдауға мүмкіндік беретін кең таралған жүйелік бағдарламалық құралдардың конфигурациясы үшін спецификациялар (шаблондар), қазіргі таңда кәсіби түрде АҚ сұрақтарымен айналысатын және АЖ аудиті Интернет қауіпсіздік орталығы (Center of Internet Security) деп аталатын халықаралық ұйым өңдеу үстінде. Қазіргі уақытқа дейін келесі

(Security Benchmarks) спецификациялары дайын немесе дайындық үстінде:

– Solaris (Level-1);
– Windows 2000 (Level-1);
– CISCO IOS Router (Level-l/Level-2);
– Linux (Level-1);
– HP-UX (Level-1);
– AIX (Level-1);
– Check Point FW-l/VPN-1 (Level-2);
– Apache Web Server (Level-2);
– Windows NT (Level-1);
– Windows 2000 Bastion Host (Level-2);
– Windows 2000 Workstation (Level-2);
– Windows IIS5 Web Server (Level-2).

Келтірілген тізімде спецификацияның бірінші деңгейі (Level-1) Internet желісіне қосылуын көптеген жүйелерге талап қойылатын қорғаудың негізгі (минималды) деңгейіне сәйкес келеді. Спецификацияның екінші деңгейі (Level-2) қауіпсіздік бойынша жоғарылатылған талаптарын қажет ететін жүйелерді қорғаудың жоғарғы деңгейіне сәйкес келеді.

Аталған спецификациялар ақпараттық қауіпсіздік облысында әлемдік тәжірибенің талқылауының нәтижесі.

АЖ компоненттерінің конфигурациясын талдау үшін бұл спецификацияларға сәйкес арнайы тестілік бағдарламалық құралдар (CIS-certified scoring tools) бар.

Мысал ретінде қорғаудың негізгі деңгейінің MS Windows 2000 ОЖ спецификациясын талдау үшін және сәйкес келетін ОЖ конфигурациясын бағдарламалық жабдықтамасын қарастырайық.

6.2.2 Windows 2000 Security Benchmark спецификациясы

CIS Windows 2000 Security Benchmark – жалпы жағдайда коммерциялық жүйелер үшін жеткілікті болатын, қорғаныстың негізгі деңгейін анықтайтын, қауіпсіздіктің минималды талаптарына MS Windows 2000 ОЖ реттеуішінің сәйкес келетінін тексеретін бағдарлама. Windows 2000 ОЖ қорғанысының негізгі деңгейінің талаптары – практикалық тәжірибенің талқылауының нәтижесі (6.1-сурет). Мұндай спецификацияларды өңдеу үшін көп көмегін тигізген SANS Institute, Center for Internet Security, US NSA и US DoD секілді ұйымдар.

CIS Windows 2000 Security Benchmark жабдықтамасының құрамына ОЖ ағымдағы реттеуішін қорғаныстың негізгі деңгейіне сәйкес қамтамасыздандыру үшін эталонды және автоматты түрде қайта конфигурациялайтын ОЖ–мен салыстыруға мүмкіндік беретін қауіпсіздік саясатының шаблоны (cis.inf) кіреді.

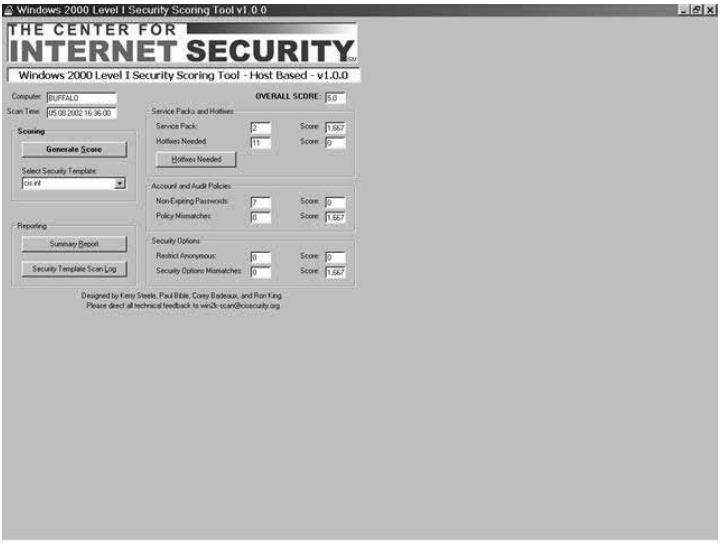
CIS Windows 2000 Security Benchmark талданатын ОЖ ағымдағы қорғаныс деңгейін 10 балдық шкала бойынша бағалауға мүмкіндік береді. 0 деңгейі қорғаныстың минималды деңгейіне сәйкес келеді (ОЖ орнатылғаннан кейін қорғаныс деңгейі 0-ге тең болады). 10 деңгейі максималды және коммерциялық жүйелер үшін талданатын жүйенің қорғаныстың негізгі деңгейінің талаптарына толық сәйкес келетінін білдіреді.

Жүйенің талдануының орындалуы барысында барлық тексерістер үш категорияға бөлінеді:

– Service Packs and Hotfixes (жаңару пакеттері және программалық түзетулері);

– Account and Audit Policies (қолданушылар бюджетін басқару саясаты және қауіпсіздік аудитінің саясаты);

– Security Options (қауіпсіздік нұсқалары).



6.1-сурет. Windows 2000 Level 1 Security Scoring Tool!

Бірінші категория (Service Packs) соңғы жаңару пакетін орнатылу тексерісін және Microsoft. атынан ағымдағы бағдарламалық түзетулерін (Hotfixes) қамтиды.

Екінші категория қолданушылар бюджетін (құпия сөз бойынша басқару саясатын қоса) басқару бойынша қауіпсіздік саясатының параметрлерін тексеруін және қауіпсіздік аудитін жүзеге асырылуын қамтиды.

Үшінші категория екі категорияға жатпайтын, ОЖ қауіпсіздіктің барлық қалған, соның ішінде анонимді сессиясына (NULL sessions) тыйым

салу, сыртқы құрылғылардың шығу ережелері, TCP/IP хаттамасының қорғау параметрлері, жүйелік объектілерге ену құқығын орнату және т.б. параметрлерінің тексерісін қамтиды.

6.3 Желілік сканерлердің мүмкіндіктері

Қауіпсіздіктің қауіп–қатерінен АЖ қорғанысын анықтайтын негізгі факторы – АЖ-дегі қорғаудың әлсіздігінің болуы. Қорғаудың әлсіздігі АЖ компонентінің конфигурациясында қателіктердің келісілуінен және тағы да басқа себептер, яғни БЖ кодында қателер және бағдарламалық бетбелгілердің болуы, қауіпсіздік механизмінің болмауы, олардың дұрыс қолданылмауы немесе тәуекелділіктерге теңбе-тең келмеуі, сонымен қатар адамдық факторлармен байланысқан әлсіздіктер болуы мүмкін.

АЖ қорғау жүйесінде әлсіздіктің болуы ақырында осы әлсіздіктерді қолдана отырып, шабуылдардың іске асырылуына әкеледі.

Желілік сканерлер қолайлы және кең қолданылатын қорғаныстыталдау құралдары болып табылады. Оның функциясының басты принципі желілік шабуылдарды іске асырып жатқан потенциалды қаскүнемнің әрекеттеріне зиян келтіру болып табылады. Мүмкін алдамшы шабуылдар арқылы әлсіздікті іздеу тексеріс тізімін жергілікті қолдану арқылы шаблон бойынша конфигурация талдауының нәтижесін толықтыратын АЖ қорғаныс талдауының тиімді тәсілдерінің бірі болып табылады. Сканер АЖ қауіпсіздігіндегі кез келген администратор немесе аудитордың ең қажетті құрал-сайманы болып табылады.

Осы заманғы сканерлер желілік сервистің кейбір немесе басқа да түрлерін көрсететін желілік қорлардың жүздеген әлсіздіктерін анықтайды. Олардың негізін қалаушылары деп 80-жылдардың басында қолдана бастаған және де қазіргі кезге дейін өзектілігін жоғалтпаған телефон нөмірлердің (war dialers) сканерлері есептелінеді. Алғашқы желілік сканерлер әртүрлі TCP-порттарын Shell тілінде сканерлейтін жай сценарийлер болатын. Қазіргі кезде олар сканерлеудің көптеген әртүрлі сценарийлерін жүзеге асыратын тәжірибелі бағдарламалық өнімге айналды.

Қазіргі желілік сканер төрт негізгі міндетті орындайды:

– қолайлы желілік қорларды сәйкестендіру;
– қолайлы желілік сервистерді сәйкестендіру;
– әлсіздіктері бар желілік сервистерді сәйкестендіру;
– әлсіздіктерді жою бойынша ұсыныс беру.

Желілік сканердің қызметіне желілік қорларға жасалған шабуылдарды жүзеге асыру үшін табылған әлсіздіктерді қолдану бойынша берілген ұсыныс қамтылмайды. Әлсіздіктерді талдау бойынша сканердің мүмкіндіктері қолайлы желілік сервис бере алатын ақпаратпен шектелген.

Сканердің жұмысының принципі host, showmount, traceout, rusers, finger, ping және т.б. тәрізді стандартты желілік утилиттердің көмегімен

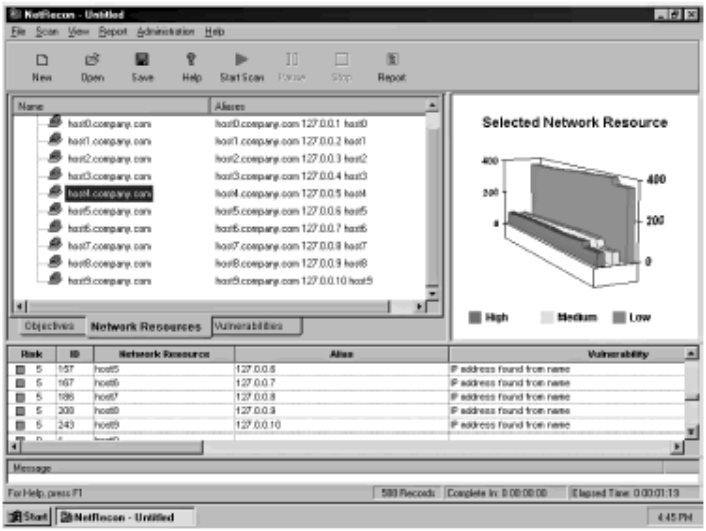
желіні талдайтын қаскүнемдердің әрекеттерін пішіндеу болып табылады. Сонымен қатар желілік сервистің, желілік хаттамалардың және ОЖ жүйелік қорларға жойылған шабуылдарды жүзеге асыру үшін белгілі әлсіздіктері қолданылады және сәтті сынақтардың құжаттамалары жүзеге асырылады.

Қазіргі таңда коммерциялық және еркін таратылатын сканерлердің, соның ішінде әмбебап және тек қана анықталған әлсіздіктер класына жататын арнайы сканерлер көп. Олардың ішіндегі көптегенін Internet желісінен табуға болады. Қазіргі сканерлердің мәліметтер қорында әлсіздіктер саны жай болса да, 1000-ға жақындады.

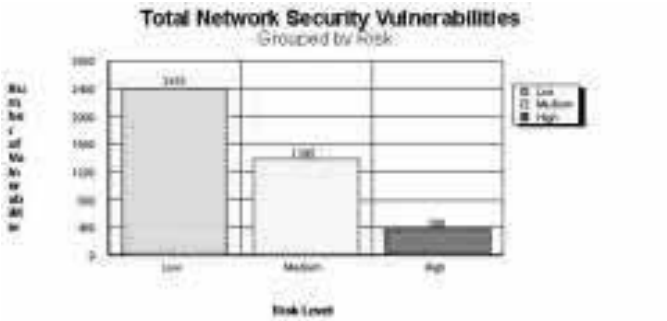
Бұл коммерциялық өнімдер класының «жоғары деңгейлілердің» бірі болып Symantec компаниясының NetRecon желілік сканері табылады, оның мәліметтер қорында 800-ге жуық UNIX, Windows және NetWare жүйелерінің әлсіздіктері бар және ол әрқашан Web арқылы жаңарып отырады. Оның қасиеттерін талқылау сол кластың барлық өнімдерінің ұғымдарымен танысуға мүмкіндік береді.

6.3.1 Symantec NetRecon сканері

NetRecon желілік сканері желі құрылымын, желілік сервисін зерттеу және желілік ортаның қорғанысын талдау үшін арналған администратордың қауіпсіздік құралы болып табылады. NetRecon желілік сервистарда, ОЖ, ЖЭ, бағыттауыштарда және басқа желілік компоненттерде әлсіздіктерді іздеуді жүзеге асырады. Мысалы, NetRecon ftp, telnet, DNS, электрондық пошта, Web-сервер және басқа желілік сервистарында әлсіздіктерді табуға көмектеседі. Сонымен қатар сервистің конфигурациясы және нұсқасы, желілік қауіп-қатерден қорғанысы және ішке ену әрекеттерінің тұрақтылығына тексеріледі. Әлсіздіктерді іздеу үшін тестілеудің стандартты құралдары, конфигурация және желінің қызметі туралы ақпаратты жинау, желілік шабуылдарды жүзеге асыратын қаскүнемдердің әрекеттеріне зиян келтіретін алгоритмдерден тұратын арнайы құралдар қолданылады.



6.- сурет. NetRecon желілік сканері



6.3-сурет. NetRecon сканерімен табылған жалпы әлсіздіктер саны

Бағдарлама Windows ОЖ ортасында жұмыс істейді және сканерлеудің нәтижелері туралы есепті қарауға және саралауға, сканерлеудің барысын бақылауға, сканерлеудің параметрлерін анықтауға мүмкіндік беретін ыңғайлы графикалық интерфейсі бар. Нәтижелер нақтылы уақыт масштабында графикалық және кестелік түрде көрсетіледі.

NetRecon құратын есептер табылған әлсіздіктер туралы, сонымен қатар қолданушылардың құпия сөздерінің төмендігі, ОЖ және басқа конфигурациясының желілік шабуылдарының осал жері үшін анықталған сервистің қауіп-қатерінен қызмет көрсетуден бас тарту туралы толық ақпараттан тұрады. Табылған әлсіздіктер және оның бейнелері туралы

хабарлармен қатар, оларды жою ұсыныстары да болады. Сканерлеудің нәтижелері туралы есеп табылған кемшіліктерді жою жоспарын құруға сілтейді.

NetRecon-да есептерді генерациялау үшін есептерді қараудың ыңғайлы амалын және оны барлық мәліметтердің форматында экспорттау үшін танымал Crystal Report БЖ қолданылады. Табылған әлсіздіктер маңызына қарай реттеледі, сканерлеу нәтижелерін талдауға жеңіл болу үшін, сыни дәрежесі бойынша сұрыптау ыңғайлы болу үшін әрқайсысы сандық рейтингке ие болады.

NetRecon-да әлсіздікті бейнелеудің келесі түрі қолданылады (алайда қалған барлық желілік сканерлерге жалпы болып қала береді):

– Vulnerability Name (әлсіздіктің атауы);

– Risk (тәуекелділік деңгейі);

– Description (әлсіздіктің бейнесі);

– Solution (әлсіздіктің жою тәсілдері);

– Additional Information (қосымша ақпарат);

– Links (белгілі әлсіздік туралы ақпарат негіздеріне сілтеме);

– of Network Resources (осы әлсіздікке тез берілгіш желілік қорлар саны);

– Network Resource (желілік қорлар тізімі).

NetRecon желі конфигурациясын өз бетімен анықтайды және сканерлеу үшін желілік қорларды таңдауға мүмкіндік береді. Барлық желілік қорлардың параллельді сканерлеу, желілік адрес диапазоны бойынша сканерлеу, жеке жүйелерді немесе желі асты сканерлеуді жүзеге асыру мүмкін. Сканерлеу сеансы қолданушының қалауы бойынша тексерістің кез келген түрі немесе жеке тексеріс жасау мүмкіндігі бар. Сканерлеу тереңдігі қолданушы тапсыратын сканерлеу ұзақтығымен анықталады. Мысалға, қолданушылардың парольдерін сөздік бойынша таңдалатын тексеріс уақытша шығындармен байланысты және сканерлеудің қысқа сеансымен бітуі мүмкін емес.

NetRecon-да желілік әлсіздіктерді табу үшін патенттелген UltraScan технологиясы қолданылады. NetRecon-да өндірілетін тексерістер бір-бірімен тығыз байланысты және бір тексерістің нәтижелері келесі біреуінің орындалуы үшін қолданылады. Жүзеге асырылатын шабуылдар жағдайындағы секілді, UltraScan технологиясында табылған әлсіздік туралы ақпарат осы әлсіздікпен байланысты басқаларын табуға қолданылады. Мысалы, егер NetRecon қолданушының құпия сөзден тұратын файлға енуді біліп алса, бірнеше құпия сөздерге қайта шифрлеу жасаса, онда бұл құпия сөздер көмегімен бұл желіге кіретін басқа жүйелерге шабуыл жасауға қолданылады.

NetRecon қолданушыға NetRecon өндірген тексерістер реттілігімен көрсетілетін әлсіздікті іздеу жолын бақылауға мүмкіндік береді. Әлсіздікті

іздеу жолы желілік қорларға шабуылды іске асырып отырған, мүмкін бұзушының әрекеттерін қадағалауға мүмкіндік береді.

Қолданылатын NetRecon мәліметтер қоры белгілі әлсіздіктер мен шабуыл сценарийлердің бейнесінен тұрады. Ол жаңа мағлұматтар үнемі толықтырылып отырады. Бұл мәліметтер қорының жаңаруы Symantec компаниясының Web-түйін арқылы LiveUpdate механизмінің көмегімен автоматты түрде жаңартылады.

6.3.2 NESSUS сканері

Nessus желілік сканері коммерциялық сканердің лайықты баламасы ретінде қарастырылады. Nessus еркін таратылатын және үнемі жаңарып отыратын бағдарламалық өнімге жатады. Ыңғайлы графикалық интерфейсі сканерлеу сеансының параметрлерін анықтауға, сканерлеу барысын бақылауға, есептерді қарауға және құруға мүмкіндік береді.

Өзінің функционалдық мүмкіндіктеріне қарай Nessus сканері алдыңғы қатарда, ал кейбір параметрлері бойынша кең таралған Symantec компаниясының NetRecon, ISS компаниясының Internet Scanner және NAI компаниясының CyberCop Scanner коммерциялық сканерлерден асып түседі.

Nessus сканерінде шабуыл сценарийі іске қосылатын модуль ретінде жүзеге асырылады. Іске қосылатын модуль саны үнемі үлкейіп отырады, қазіргі таңда 700 санына жеткен. Шабуылдарға зиян келтіретін жаңа сыртқы модульдерді Web-серверін өңдеушілерден бастапқы текстері бар файлдарды көшіру арқылы орнатуға болады (www.nessus.org).

Nessus сканері бірлескен желінің әлсіздіктерін іздеу және желілік сервистің құрылымын зерттеуге кең мүмкіндік береді. Nessus TCP және UDP порттарын сканерлеудің стандартты тәсілін қолданып қана қоймай, ICMP және SNMP желілерін басқаратын хаттамаларды жүзеге асыруда әлсіздіктерді іздеуге мүмкіндік береді. Одан басқа Nessus сканерінің компоненттерінің бірі ретінде қарастырылатын, атақты коммерциялық емес nmap стелс-сканерімен жүзеге асырылатын сканерлеудің әртүрлі стелс-режимдерін қолдайды. Атақты queso коммерциялық емес сканері Nessus құрамында ОЖ-мен сканерленетін нұсқау нөмірін және типін анықтауға қолданылады.

Сканерлеудің жоғарғы жылдамдығына желілік хосттарды біруақытта параллельді сканерлеуге мүмкіндік беретін, бағдарламаның көпағымды архитектурасын қолдана отырып, Nessus сканерін жүзеге асырғанда көтеріледі.

Әрбір хостты nessusd серверімен сканерлеу үшін орындалудың жеке ағымы пайда болады.

TCP/UDP порттарын сканерлеу үшін қолданылатын әдістердің толық бейнесін nmap сканерінің құжаттамасында табуға болады. Оларға мыналар жатады:

– TCP connect scan;
– TCP SYN scan;
– TCP FIN scan;
– TCP Xmas Tree scan;
– TCP Null scan;
– UDP scan.

Nessus-ті іске асыру үшін, желілік сканерлер үшін типтік емес клиент-серверлік архитектурасы пайдаланылған. Клиент пен сервер арасындағы өзара әрекеттесу сенімді аутентификация схемасын қолдануды және жіберілетін мәліметтерді шифрлеуді қарастыратын қорғалған клиент-серверлік хаттама арқылы жүзеге асырылады. Nessusd сервері UNIX ортасында жұмыс істейді және сканерлеудің сценарийін орындау үшін арналған. Nessusd серверінде іске асырылған өзіндік қауіпсіздіктің механизмі қолданушылардың сканерлерін аутентификациялауға, сканерлеудің орындалуы бойынша қолданушылардың өкілеттілігін шектеуге және сервердегі оқиғаларды тіркеу журналына қолданушылардың барлық әрекеттерін тіркеуге мүмкіндік береді.

Nessus-тің клиенттік бөлігі UNIX және Windows ортасында жұмыс жасайды және nessusd серверін басқару үшін қолданушының графикалық интерфейсі жүзеге асырады. Сканерді қолданушы сканерлеу сеансы басталмас бұрын, сканерленетін IP-адрестер мен TCP/UDP-порттардың диапазонын көрсететін сканерлеу параметрлерін, сканерлеу ағымының максималды санын (біруақытта сканерленетін хосттар саны), қолданылатын сканерлеудің сценарийін және әдістерін анықтап алады.

Сканерлеудің барлық сценарийлері әлсіздіктерді табатын желілік шабуылдармен жүзеге асырылатын түрі бойынша және де тестіленетін желілік сервистің түрі бойынша екі топқа бөлінеді. Сценарийдің арнайы топтары бар:

– Backdoors - «трояндық» бағдарламаларды табу үшін;
– Gain Shell Remotely – жоғалған UNIX-жүйесінде қолданушылардың өкілеттілігін алу үшін шабуылды жүзеге асыру;
– Firewalls – ЖЭ тестілеу үшін;
– FTP-серверлерді тестілеу үшін;
– Windows-жүйесінің әлсіздіктерін іздеу үшін.

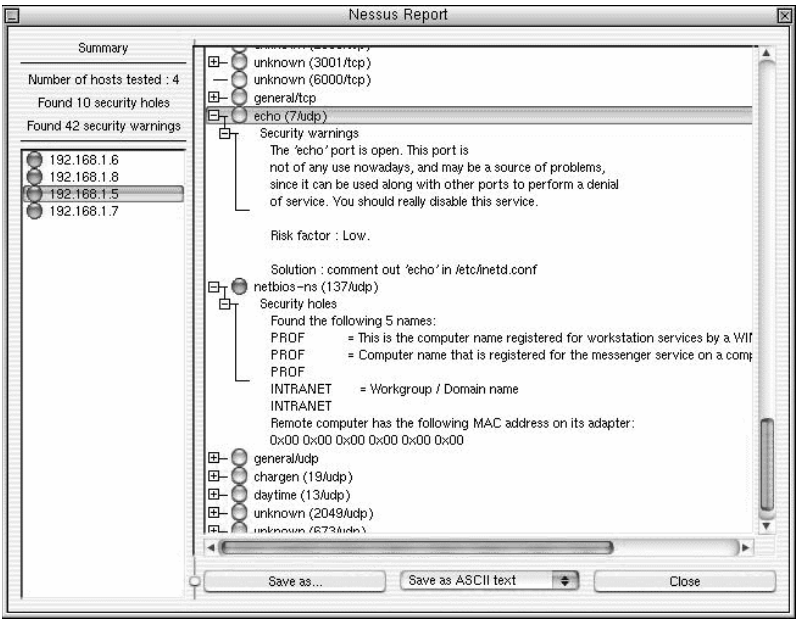
Сканерлеу сценарийнің ерекше тобын «қызмет көрсетуде қабыл алмау» шабуылдары құрайды (Denail of Service-DoS). Сканерленетін жүйенің кейбір немес басқа DoS сценарийіне шалдыққанын білу үшін, шабуылды орындап және жүйенің реакциясын қарау қажет. Алайда бұл сценарий тобы өте қауіпті, өйткені олардың жіберілуі сканерленетін желіде күт-

пеген жағдайларға әкелуге, жұмыс станцияларында және сервер жұмысында жаңылдыруы немесе бірлескен желіні толықтай құртып және мәліметтерді жойып жіберуі мүмкін. Сондықтан көптеген DoS осы топтарда үнсіз келісім бойынша ажыратулы тұрады.

Шабуылдар сценарийін жазу үшін NASL (Nessus Attack Scripting Language) жоғары деңгейлі бағдарламаның арнайы C-тәрізді тілі қызмет етеді. Сонымен қатар C тілінде шабуылдар сценарийімен іске қосылатын модульдерді өңдейтін (API) қолданбалы бағдарламаның интерфейсі бар, алайда NASL қолданған жөн.

NASL платформадан оның тәуелсіздігін қамтамасыз ететін өзінше түсіндірілетін бағдарламалау тілі. Ол IP-пакеттерді пішіндеудің еркін түрін талап ететін желілік өзара әрекет үшін кез келген сценарийді іске асыратын мықты құралдарды көрсетеді.

Nessus сканерінің жұмыс нәтижесі 6.4-суретте көрсетілген. Табылған әлсіздіктер сканерленген хосттардың IP-адрестері бойынша сұрыпталған. Табылған әлсіздіктер маңызы бойынша реттелді. Ең ерекше сыналғаны (security holes) қызыл түспен, ең аз сыналғаны (security warning) сарымен ерекшеленген. Әрбір әлсіздік бойынша оның бейнелеуі, ассоциацияланған Risk Factor тәуекелділікпен бағалау және оны жою бойынша ұсыныстар келтіріледі (Solution).



6.4-сурет. Nessus сканеріндегі сканерлеу нәтижелері

6.4 Жүйелік деңгейдің қорғанысының бақылау құралдары

Компьютерлік жүйенің қауіпсіздігін қамтамасыз ету көптеген мүмкін болатын қауіп-қатерді анықтау, тәуекелділіктермен байланысты мәндерді бағалау, адекватты контмерді таңдау, бұл контрмерлерді процедуралық және бағдарламалы-техникалық құралдар арқылы жүзеге асыру болып табылады.

Соңғы сұрақ қиындардың бірі болып табылады. Қорғаудың бағдарламалық-техникалық шараларын жүзеге асыру активті желілік жабдықтаманың және қолданбалы бағдарламалардың, МҚБЖ, желілік сервис, ОЖ-ның көптеген параметрлерінің реттелгенін талап етеді. Жеке сервер немесе жұмыс станциясын қорғау туралы тақырып қозғалғанда, оның тапсырмасы қиын болып көрінеді, алайда тәжірибелі жүйелік администраторына оның шешімі оңай болып көрінеді. Бұл жағдайда қауіпсіздікпен байланысты бағдарламаның параметрінің мәндерін бақылау үшін арнайы тексеріс тізімі қолданылады. Егер реттейтін әртүрлі бағдарламалық-аппараттық платформада қызмет атқаратын желілік құрылғының саны ондаған немесе жүздеген болса, ортақ қауіпсіздік саясатына қорғаудың параметрінің бақылауы және шын масштабты уақытында қауіпсіздіктің мониторингіне сәйкес болғандықтан, автоматизацияның арнайы емес құралдарынсыз істеу қиын. ОЖ өндірушілері ОЖ қорғанысын талдау және бүтіндігін бақылау үшін арнайы құралдарды ұсынады (Windows NT Resource Kit жүйесінде C2 Configuration утилитасы, Solaris жүйесінде ASET утилитасы және т.б.). Осындай есептерді шешетін еркін таралатын және кең қолданылатын UNIX ОЖ ортасына арналған COPS бағдарламасы секілді өнімдері бар. Алайда желілік деңгейдегі қызмет ететін бұл құралдары кейбір өз ОЖ қорғанысының базалық деңгейін қамтамасыз етуге мүмкіндік береді. Қосымшаны бақылау, желілік сервистерді, динамикалық агрессивті ортада қызмет ететін үлестірілген жүйелердегі активті желілік жабдықтамаларды бақылау үшін үлестірілген архитектураны қолдайтын, алгоритмнің ізденісін және әлсіздіктерді жоятынын жүзеге асыратын, қорғаудың басқа құралдармен интеграцияланған және бұл кластың өніміне қойылатын талаптарды қанағаттандыратын қосымшаның әртүрлі түрлері, арнайы құралдарды қолдану қажет.

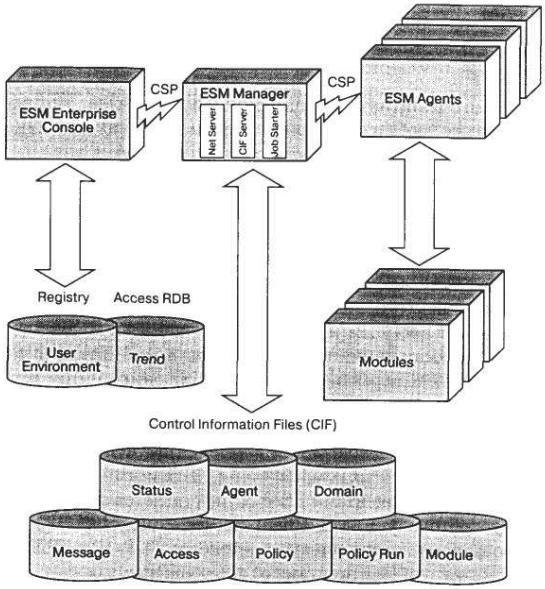
6.4.1 Symantec Enterprise Security Manager(ESM) жүйесі

Жүйелік деңгейдің қорғаныс талдауының мықты құралы ОЖ конфигурациялы параметрлерін және «іштей» қосымшасын тексеруін орындайтын Symantec компаниясының ESM өнеркәсібінің қауіпсіздікпен автоматты басқару жүйесі болып табылады. ESM бағдарламалық агенттері қажетінше түзелетін қауіпсіздікпен байланысты БЖ параметрлерінің тексерісін жүргізетін желінің әрбір бақыланатын компьютерінде орнатылады. Бағдарламалық агенттер БЖ параметрлерін талдау үшін өте қиын тексеріс-

терді жүргізе алады, өйткені олар іштей желілік сканерлердің ене алмайтын бөлігінде қызмет етеді. Бағдарламалық агенттердің көмегімен жүргізілетін қорғаныс талдауы уақыт бойынша жоспарланады және біруақытта барлық бақыланатын компьютерлерде орындалады. Одан басқа желілік сканерлерге қарағанда бағдарламалық агенттер желінің ену амалына әсер етпейді және желі бойынша мәліметтерді жіберу кезінде нәтижелерді шифрлеу мүмкіндігі бар.

ESM жүйесі консоль/менеджер/агент архитектура бойынша құрылған. Ол желі бойынша еркін тартылатын үш типті компоненттерден тұрады: административті консоль (ESM Console), менеджерлер (ESM Manager) және агенттер (ESM Agent). 6.5-суретті қараңыз.

Административті консоль менеджерлерді басқару үшін қолданылатын графикалық қолданбалы интерфейс және өз қызметін Windows NT ортасында атқарады. Менеджерлерді басқару үшін сонымен қатар (CLI) интерфейстің командалық жолы қолданылады.



6.5-сурет. ESM архитектурасы

Административті консоль келесі тапсырмаларды орындауға арналған:

– ESM-менеджерде қолданушылардың тіркелген жазбаларымен басқару;

– ESM жүйесінде қолданушы өкілеттілігін анықтау;

– ESM-менеджерден желі жағдайы туралы ақпаратты талдау және жинау;

– Бақыланатын жүйенің қорғаныс деңгейін анықтау және әлсіздікті маңызына қарай реттеу;

– Қауіпсіздік саясатын өзгерту және құру;

– Бақыланатын домендерде қауіпсіздік саясатын жүзеге асыру;

– Тексерістің орындалу кестесін орнату;

– Орындалған тексерістің нәтижелерінің кестелік және графикалық түрде бейнеленуі;

– Орындалған тексерістің нәтижелері бойынша шолу және генерациялау;

– ОЖ кейбір параметрлерін түзету.

ESM-менеджер жүйенің орталық компоненті болып табылады. Ол негізгі екі қызметті атқарады:

– қауіпсіздік саясаты туралы мәліметтерді сақтайды және осы мәліметтерді басқарады, сонымен қатар административті консольге және агенттерге мәліметтерді жібереді;

– орындалған тексеріс нәтижелері туралы мәліметтерді басқару жүзеге асырылады, ESM-агенттерден осы мәліметтерді алады және оларды административті консольге жібереді;

Менеджердің негізгі компоненті – мәліметтермен басқарылатын CIF-сервер. ESM қолданушылар туралы барлық мәліметтер, өкілеттіліктері, агенттері, домендері, қауіпсіздік саясаты, тексеріс нәтижесі және шаблондары, сонымен қатар агенттерден түскен хабарлары басқарылатын ақпарат файлында сақталады. Ол административті консольдің және интерфейстің командалық жолының сұранысына қажетті ақпарат береді. CIF-сервер сұранысты менеджерлердің басқа компоненттеріне орындауға бағыттайды. Мысалы, есеп менеджеріне (Job Starter) домендегі қауіпсіздік саясатын орындауының жүзеге асырылу қажеттілігі туралы хабарлайды. Желілік сервер (Net Server) жойылған агенттердің CIF-сервері мен басқа да компоненттерімен байланысын қамтамасыз ететін менеджердің тағы да бір компоненті болып табылады. ESM таратылған компоненттерінің арасындағы байланыс желілік TCP/IP мен SPX/IPX хаттамаларының үстінен жүзеге асырылған қолданбалы деңгейдің ESM's Client Server Protocol (CSP) қорғалған клиент-серверлік хаттамасы арқылы орнатылады. Менеджерлер мен агенттер арасындағы трафиктің қорғанысының тыңдалуы DES американдық стандартты шифрлаудың жетілген нұсқасы болып табылатын DESX алгоритмі бойынша шифрлеу жүргізіледі.

ESM агенттері менеджерлер секілді модульдік құрылымға ие. Олар серверлік бөліктен, қауіпсіздік модулінен және байланыс құралдарынан тұрады. Олар жүйенің қауіпсіздігі туралы ақпарат жинайды. Ақпаратты талдау және жинақтау менеджерлерден қауіпсіздік саясатын іске қосу туралы бұйрығы түскен кезден басталады. Агенттің серверлік компоненті қауіпсіздік модулінің тексерісінің нәтижесі туралы мәлімет жинайды және

оны менеджерге жібереді. Агенттер бірқатар басқа да маңызды қызмет атқарады:

– жүйенің жағдайы және қолданушылар бюджеті туралы мәліметтерден тұратын лезде түсірілімдерді сақтайды;

– жүйенің жағдайының лезде түсірілімдерін жаңартып отырады;

– қолданушылардың сұранысы бойынша жүйенің кейбір параметрлеріне түзетулер енгізеді.

ESM қауіпсіздік саясаты қауіпсіздік модулінің жиынтығын көрсетеді. ESM қорғаныстың әртүрлі деңгейін қамтамасыз ететін алдын ала анықталған қауіпсіздік саясатының жиынтығынан тұрады. Кәсіпорынның қауіпсіздік саясаты ESM алдын ала анықталған қауіпсіздік саясатының негізінде санын және олармен жасалған тексерістің мазмұнын өзгерту мақсатымен қауіпсіздік модулін реттеу жолы арқылы асырылады. Агенттердің домендік ұйымдары қауіпсіздік саясатының әрекеттерін жеке жүйелерге, жүйелік топтарға және түгел кәсіпорынға таратуға мүмкіндік береді.

Бақыланатын жүйелер қауіпсіздік саясатының тағайындалған ережелер жиынтығына сәйкес келуі міндетті. ESM жүйенің қорғанысының талдауын қауіпсіздік саясаты тағайындаған конфигурационды параметрлерінің олардың мәндерімен салыстыру арқылы жүргізеді. ESM сыни деңгейі бойынша тексеріс нәтижелерін маңызы бойынша реттеуді және табылған әлсіздіктердің сандық рейтингтерін қоса отырып, жүйенің жалпы қорғаныс деңгейін анықтауды орындайды.

ESM бастапқы конфигурациялау тапсырмасын тексеріс тереңдігі мен өсу ретімен түгенделетін алдын ала анықталған қауіпсіздік саясаты жеңілдетеді:

– Phase 1;

– Phase 2;

– Phase 3:a Relaxed;

– Phase 3:b Cautious;

– Phase 3:c Strict.

Бірінші деңгей саясаты (Phase 1) көптеген жүйелердің қорғаныс деңгейі үшін минималды қажетті кедергілерді жоюды қамтамасыз ететін әлсіздіктің өте маңызды және потенциалды қауіпті түрін тексеруге арналған қауіпсіздік модулін қамтиды.

Екінші деңгей саясаты (Phase 2) ESM қауіпсіздік модуліндегі барлық өте маңызды тексерістің тек қана іске қосылған негізгі түрлерін қамтиды.

Үшінші деңгей саясаты (Phase 3) мыналарды қамтиды:

– Екінші деңгеймен бірдей негізгі нұсқаусын (Relaxed);

– Тексерістің қосымша түрінен тұратын жақсартылған нұсқаусын (Cautious);

– Белгілі ОЖ-ні қолдайтын барлық қауіпсіздік модуліндегі тексерістің барлық түрінен тұратын күшейтілген нұсқасын (Strict).

Аталғандардан басқа ESM-де бірнеше арнайы қауіпсіздік саясаты бар. Алдын ала анықталған Queries қауіпсіздік саясаты ESM және ITA агенттері орнатылмаған жүйелер, топтар және қолданушылар туралы ақпаратты беретін тек қана ақпараттық модульдерін қамтиды. Ол NetWare мен Windows платформаларына арнайы өңделген.

Арнайы NetRecon саясаты ESM-консолінің сканерлеу құралдарының нәтижелерін талдауға және қарауға мүмкіндік беретін, Windows платформасында NetRecon сканерімен бірігуі үшін қолданылады. Ол ESM хабарлау пішінінде NetRecon сканерімен генерацияланған әлсіздіктер туралы жазбаларды қайта жаңартуды жүзеге асырады.

Бірлескен желінің қорғаныс бақылауы ESM көмегімен ақпараттық жүйеге ұсынылған қауіпсіздіктің талаптарының қатаңдау жолымен жүргізіледі. Бақыланатын жүйедегі іске қосылатын саясаттың бірінші және екінші деңгейінен бастаған жөн. Көптеген коммерциялық жүйелер үшін қорғаныстың мұндай деңгейі өте қолайлы. Барлық тексерістің жақсы өткізілуіне байланысты, ерекше сыни жүйелерінде қорғаныс параметрлерінің терең талдауы үшін қауіпсіздік саясатының үшінші деңгейін жүзеге асыруға болады.

Алдын ала анықталған қауіпсіздік саясаты негізінде ұйымның талаптарына сай келетін жеке өзіндік саясат құруға болады. Қауіпсіздік саясатын құру үшін ESM құрамында бағдарламаны толық қоспайтын графикалық құралдар бар.

ESM-агенттер модулі – қауіпсіздік саясаты ұсынылған тексерістерді жүргізетін бағдарламалық модульдер. ESM модульдерінің екі түрі бар: қауіпсіздік модулі және сұраныс модулі. Біріншісі авторизация параметрлерін және қолданушы бюджетін басқару, сервер параметрлерін және желілік параметрлерді реттеу, каталогтар және файлдық жүйелердің атрибуттарын қамтитын қауіпсіздіктің әртүрлі облыстарын бақылайды. Екіншісі жүйенің жағдайы туралы ақпаратты жинақтау үшін арналған. Мысалға, анықталған топқа кіретін қолданушылар тізімін алу немесе административті өкілеттілігімен бөлінген қолданушылар.

Ақпараттық модульдер қауіпсіздіктің басқару тапсырмаларын орындалу кезіндегі жүйенің әртүрлі параметрлері туралы ақпарат жинау үшін қызмет етеді. 6.1 кестесінде кейбір ақпараттық модульдер сипаты көрсетілген.

6.1.-кесте

ESM ақпараттық модульдері

Модуль атауы	Сипаты
Account Information	Бұл модуль ОЖ қолданушыларының тіркелген жазбалары туралы ақпарат алуға арналған. Windows NT ортасында қолданушылардың өкілеттілігі туралы ақпаратты, администратор құқығы бар қолданушылар тізімін, қолданушылардың тіркелген кілттенген және өшірілген жазбалар тізімін, әрбір топқа кіретін топ тізімін және қолданушылар тізімін қайтарады. NetWare ОЖ-де модуль әрбір топқа кіретін топ тізімін және қолданушылар тізімін, қауіпсіздік баламасын, енудің тиімді құқығын, сенімділік қатынасын қайтарады.
Discovery	Бұл модуль TCP-порттарды (белсенділерді шығару мақсатымен) сканерлейді, желілік қорларды сәйкестендіру және ESM және ITA бағдарламалық агенттердің бақылауындағы емес хосттар тізімін құруға тырысады.
File Information	NetWare ОЖ-не арналған файлдарға кіру параметрлер тізімін қайтарады.

Қауіпсіздік модулін тағайындау:

– жүйеге кірген кездегі қолданушылардың идентификациясы, аутентификациясы және авторизациясы, құпия сөздер мен қолданушы бюджетін басқару;

– желілік хаттамаларды және сервистерді конфигурациялау;

– файлдарға және каталогтарға енуді басқару.

Қолданушы белгіленген модуль ішінде қолайлы тексерісті таңдау мүмкіндігі бар. Әрбір тексеріс әлсіздіктің кейбір типін жүзеге асырады. Мысалы, Login Parameters модулінің құрамына кіретін тексерістер жүйеде тіркелген, бірақ әрекет уақыты өтіп кеткен белсенді емес қолданушыларды және жүйеге кіруді бірнеше сәтсіз сынақтар санын шектеулігін орнатуға мүмкіндік береді. Қауіпсіздіктің модульдерінің бірқатары анықталған ОЖ параметрлерін және қосымшаларын тексеру үшін қолданылады, ал кейбіреулері әмбебап түрлері бірнеше ОЖ қамтиды. 6.2 кестесінде қауіпсіздіктің негізгі модульдері сипатталған.

6.2-кесте

ESM қауіпсіздік модульдері

Қауіпсіздік модулі	Сипаты
Account Integrity	Қолданушылардың талғампаздығы, парольдермен басқару және қолданушылардың тіркеу жазбалар саясаты тексеріледі
Backup Integrity	Резервтік көшірудің жүйе бөлігінің параметрлері тексеріледі, резервтік көшірмелері құрылмаған файлдар шығарылады
File Access	Файлдардың ену құқығының қауіпсіздік саясаты орнатқан ережелерге сәйкестігі тексеріледі
File Attributes	Мәліметтік файлдардың атрибуттарының бүтіндігін бақылау
File Find	Файлдардың бүтіндігі және файлдарды вирустардың бар болуына жасалған бақылауы тексеріледі
Login Parameters	Жүйедегі тіркеу параметрлерін орнатылған қауіпсіздік саясатының ережелеріне сәйкестігін тексеріледі
Object Integrity	Ие болу құқығының өзгеруі, орындалатын файлдардың басқа атрибуттарын және кіру құқықтары бақыланады
Password Strength	Қолданушылар парольдері парольдермен басқару саясатымен тағайындалған ережелеріне сәйкестігі тексеріледі. «Осал» құпия сөздер және мүлдем жоқ құпия сөздер шығарылады.
Startup Files	Жүйені жүктеу кезінде орындалатын командалық файлдарды әлсіздікке тексереді
System Auditing	Аудит жүйе бөлігінің параметрлері тексеру және Windows аудит журналының мониторингін жүзеге асыру
System Mai	Қауіпсіздікпен байланысты электрондық пошта жүйесінің конфигурациялы параметрлері тексеріледі
System Queues	сгоп, patch және at UNIX ОЖ жүйелік утилиттерінің кезегін реттеу параметрлерін, сонымен қатар OpenVMS ОЖ жүйе бөлігінің спулинг параметрлері тексеріледі
User Files	Қолданушылардың ие болу құқығы және файлдарға кіру құқығы тексеріледі
Registry	Windows ОЖ реестрінің кілттерінің атрибуты және кіру құқығы тексеріледі
Network Vulnerabilies	NetRecon желілік сканерімен табылған желілік параметрлерінің реттеуішінің әлсіздігі талданады

Қауіпсіздікпен басқару жұмысын жеңілдету мақсатында ESM көмегімен ESM агенттері домендерге біріктіріледі. ESM домені деп белгілі бір белгі бойынша біріктірілген агенттер тобын атаймыз. Барлық агенттер үнсіз келісім бойынша доменге операциялық жүйе типі бойынша біріктірілген. Осылайша, бастапқыда Windows-домен, UNIX-домен, NetWare-домен және OpenVMS-домен болады. Домендік ұйым кәсіпорынның ұйымдастырылған және территориялық құрылымын бейнелейді.

Тексеріс барысында ESM қауіпсіздік саясатының бұзылғандығына ізденіс орындайды. Қауіпсіздік саясатының бұзылымының екі типі болады:

– қауіпсіздік саясатының ережелеріне сай келмеу;

– жүйенің ағымдағы жағдайының соңғы жасалған алдыңғы тексеріс кезінде сақталған лездік түсіріліміне сәйкес келмеу.

Лездік түсірілімдер ESM-де ОЖ және қосымшалардың ақпараттық бөлігін және бағдарламаның бүтіндігі бақылау және жүйенің конфигурациясында өзгерістерді қадағалау үшін қолданылады. Лездік түсірілімдер ожы жүйеге тән құру және модификация уақыты, тексеру сомасы және файлдар кіру құқығы тәрізді объектілердің атрибуттарының мәндерінен тұрады. Лездік түсірілімдері бар файлдар бақыланатын жүйедегі қауіпсіздік саясатының бірінші қосылыс кезінде құрылады. Келесі қосылыстар кезінде жүйенің жағдайының лездік түсірілімдері алдыңғысымен салыстырылады, жүйелік объектілерінің атрибуттарында және конфигурация параметрлерінде пайда болған айырмашылықтар потенциалды әлсіздіктер ретінде қарастырылады. Объектілердің жағдайлары лездік түсірілімдермен салыстырылып отырады, барлық айырмашылықтар туралы хабарламалар менеджерлерге жіберіледі, ал олар қауіпсіздіктің мәліметтер қорына жазылады.

ESM әрбір агенті File, User, Group, Device аты бар лездік түсірілімдердің бірнеше файлдарын құрады. User, Group және Device файлдары жүйелік объектілердің сәйкес келетін жағдайы туралы ақпарат береді. User файлы қолданушы бюджеті, соның ішінде қолданушы өкілеттілігі мен қолданушының артықшылықтарынан тұрады. Group файлы қолданушылар тобын, соның ішінде топ үшін өкілеттік және артықшылықтар, сонымен қатар топтың мүшелерінің тізімінен тұрады. Device файлы иеленушінің атынан, ену құқығынан және құрылғылардың атрибуттарынан тұрады.

Басқа лездік түсірілімдерден File-дың айырмашалығы, ол файлдардың өзгерісінде күдікті тексеріс, вирустарға және «трояндық» аттарды табу мақсатында арнайы шаблондармен салыстыру үшін қолданылады.

Қосымша Oracle modules, Web modules және т.б. агенттерге орнатылатын қауіпсіздіктің арнайы модульдері лездік түсірілімдердің жеке түрлерін жасауы мүмкін.

Шаблондар қауіпсіздік саясатының ережелеріне жүйенің конфигурациясының сәйкес келмегендіктерін анықтау үшін қолданылады. Олар жүйелік объектілердің тізімін және жағдайын баяндайды. File Attributes модулі Windows 2000 Professional ОЖ жүйелік файлдарының атрибуттарын (fileatt.w50) шаблоны бойынша, ал модуль OS Patches ОЖ үшін орнатылған бағдарламалық түзетулердің бар болуын (patch.pw5) шаблон бойынша тексереді.

ESM бәсекелесетін өнімдердің ішіндегі ірі және тез көтерілетін желілерге қолданған жөн, өйткені кең ауқымдылықтың жақсы сипаттамаларына ие. Басқарушы консоль ESM 5.0 нұсқасы 40 менеджер мен 10000 агентті қолдай алады. ESM-менеджері Pentium 120 МГц немес SPARC 276 МГц процесінде 400 агентке дейін қолдайтын мүмкіндігі бар. Басқарушы консолі өз қызметін әртүрлі графикалық, сонымен қатар X-Window, Windows 3.x, Windows 95/98/NT ортасында атқарады. Қазіргі таңда ESM ОЖ және қосымшасының реттеуіш параметрінің тексерісі 1000-ға жуық. 55 әртүрлі өнім қолданылады, соның ішінде ОЖ, бағыттауыштар, ЖЭ, Web-серверлер, МҚБЖ Oracle және Lotus Notes. ОЖ қолдайтындардың әртүрлі нұсқалары бар UNIX, Windows NT, NetWare, OpenVMS және т.б.

ESM мүмкіндіктері жаңа қосымшаларды қолдауды қамтамасыз ету мақсатында кеңейтілуі мүмкін. Бағдарламалық құрал ESM SDK МҚБЖ серверлері, Web-серверлер пошталық серверлер, ЖЭ және т.б. секілді жаңа қосымшаларды қолдау үшін қауіпсіздіктің жаңа модульдерін құруға мүмкіндік береді. Жаңа модульдерді өңдеу ESM API кітапханалық қызмет көмегімен жүзеге асырылады. Қазіргі таңда ISO 17799 стандартының талабына сай ОЖ қауіпсіздік саясаты, сонымен қатар NAV Corporate Edition 7.6 серверлік бөліктің бақылауына арнайы антивирусты саясаты құрылған.

АЖ қызметінің әртүрлі аспектілерін және қосымшалардың әрқилы түрлерін бақылау үшін арналған қауіпсіздік саясатының саны үнемі ұлғаюда. ESM қауіпсіздік модулінің және қолайлы саясатының тізімін мына Web-сайттан Symantec Security Response Team: http://securityresponse.symantec.com/. тауып алуға болады.

ESM құрамына HP OpenView және IBM (Tivoli ортасы) желілік басқарудың құралдары мен интеграциялауға арналған арнайы модульдер кіреді.

Барлық артықшылықтарына қарамастан, бағдарламалық агенттердің қолдану желілік сканерді алмастыра алмайды, сондықтан оны желілік сканермен бірге қолданған жөн.

V I I ТАРАУ

ШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ТӘУЕКЕЛДЕРМЕН БАСҚАРУ

Тәуекел ұғымы адамдық қызметтің кез келген аймағында қолданылады. Адам баласы қандай қызмет түрімен айналыспасын, сол қызметінің мақсатына белгілі бір себептермен жете алмай қалу ықтималдығы әрқашан болып тұрады. Адамның тіршілік етуінің өзі тәуекелге барудан тұрады және біз сол тәуекелге бел байлағанымыздың кесірінен біраз қауіпті зиян шегуіміз мүмкін. Осылайша, *тәуекел зиян шегу мүмкіндігі деп түсіндіріледі.* Біз өмір бойы біліп немесе аңдаусыз әртүрлі тәуекелдерді бағалаумен айналысамыз: жолдан өтіп жатып, теңгені долларға ауыстырғанда немесе дискін дискжетекке салып жатып.

Ақпараттық қауіпсіздік сферасында тәуекелді бағалау адамдық қызметтің басқа да барлық аймақтарындағыдай бірінші орында тұрады. Ақпараттық қауіпсіздіктің қаупінің іске асуымен байланысты тәуекелді дұрыс бағаламаудың кесірінен, қазіргі замандық жоғарғытехнологиялық ортада мемлекет, ұйымдар мен жеке тұлғалар, оны есептеу ешкімнің қолынан келе қоймайтын, күрделі шығынға ұшырайды.

Тәуекелдің мөлшері қауіптің болу ықтималдығымен және нәтижесінде кесірі тиетін зиянның мөлшерімен анықталады. Мүмкін болатын зиян әрқашан ақша бірлігінде болмауы да мүмкін, ал қауіптің іске асу ықтималдығын нақты бағалау мүмкін емес. Сондықтан, біздің тәуекелді бағалауымыз тек жуықтап қана болып табылады. Олардың нақтылығы біздің ағымдағы жағдайдан қаншалықты жақсы хабардар болуымызға, қауіпті іске асырудың әдістері мен табиғатын дұрыс болжай алуымызға және де біздің олардың зардаптарын бағалау және қорытындылай білу қабілеттілігімізге байланысты.

Тәуекелдерді бағалап болып, олармен не істеу керектігін шешу қажет. Бұл үрдіс тәуекелдермен басқару деп аталады.

Тәуекелмен басқарудың міндетіне тәуекел мөлшерін қажетті мөлшерге дейін азайтуға мүмкіндік беретін қарсы әдістерді таңдау және сол таңдауды негіздеу кіреді. Қарсы әдістерді қабылдаудың құны мен мүмкін болатын зиян мөлшерінің айырмашылығы зиян тигізу ықтималдығы қаншалықты аз болса, соншалықты көп болуы тиіс.

Қарсы әдістер тәуекел деңгейін әртүрлі әдістермен төмендете алады:

- қауіпсіздік қаупінің іске асуының ықтималдығын төмендете отырып;

- осалдықтарды жою немесе олардың мөлшерін төмендете отырып;

- мүмкін болатын зиянның мөлшерін төмендете отырып;

- зияны тиген автоматтандырылған жүйе қорларының қайта қалпына келуіне жағдай жасай отырып;

- шабуылдар мен басқа да қауіпсіздікті бұзуларды анықтай отырып.

Бұл бөлімде шабуылдарды анықтауға қатысты сұрақтар кешені қарастырылады.

7.1 Желілік шабуылдар

Дүниежүзілік экономика мен мемлекеттік құрылымдардың Internet-тен тәуелділігі артқаннан бастап Internet-ке қосылған желінің кешендеріне жасалатын желілік шабуылдармен байланысты тәуекел мөлшері де артып келе жатыр. Ауқымды желіден жасалатын шабуылдар мемлекеттер арасындағы ақпараттық соғыстар жүргізудің, лаңкестік актілерді де қоса, қаржылық және басқа да сферадағы қылмыстарды жасаудың қуатты қаруы болып келе жатыр. 2001 жылдың 22 қыркүйегінде Американың қауіпсіздікті қамтамасыз ету технологияларын зерттеу институты (Institute for Security Technology Studies At Dartmouth College) «Лаңкестікпен соғыс кезіндегі кибер шабуылдар» (Cyber Attacks During The War on Terrorism: A Predictive Analysis) атты есеп беруді баспаға шығарды. Бұл есеп берудің ішінде Internet-қорларына желілік шабуылдардың санының артуын саяси дау-дамайлар ынталандыратын жағдайлардың талдауы бар. Осындай көзқараспен Үндістан мен Пәкістан, Израиль мен Палестина, NATO мен Сербия, АҚШ пен Қытайдың қытайлық құртушы мен американдық тікұшақ-барлаушысының соқтығысының кесірінен болған араларындағы дау-дамайлар зерттелді. Қамданылған зерттеудің мақсаты 2001 ж. 11 қыркүйегінде болған қайғылы оқиғадан кейінгі АҚШ-та кең ауқымды лаңкестікке қарсы науқанның жүргізілуінің нәтижесінде жағдайды Internet-те болжау болып табылады. Бұл зерттеуде шабуылдың объектісі ретінде АҚШ-тың иелігіндегі Internet-қорлар қарастырылды, шыққан нәтижелер Ресейді қоса алғанда басқа да барлық мемлекеттерде қолданылады.

Желілік шабуылдардың потенциалды қайнар көздері келесі топтарға бөлінген:

- лаңкестік топтар;

- лаңкестердің іс-әрекеттерін қолдайтын немесе АҚШ-қа қарсы тұрмайтын хакерлер;

- АҚШ-тың лаңкестікке қарсы науқаны (Ауғанстан, Сирия, Иран, Ирак, Судан және Ливияны қоса алғанда) қарсы шығуы мүмкін дүниежүзілік лаңкестіктің қорғаны болып есептелетін мемлекеттер;

- қызығушылығы мол және өзінің біліміне сенімді хакерлер.

Желілік шабуылдардың басты мақсаты ретінде талқыланғандар:

- АҚШ және одақтас елдерде Web-серверлердегі (Web defacing) беттерді ауыстыру, жалған ақпараттарды және насихаттарды тарату;

- АҚШ және одақтас елдердегі желілік құрттар мен вирустардың қолданылуымен желілік АҚ-тың әлсіз жерлеріне, ақпараттық инфражүйенің маңызды бөлшектеріне «қызмет көрсетуден бас тарту» (DoS) шабуылдарының жасалуы;

- нәтижесі ақпараттық инфражүйенің маңызды бөлшектерінің зақымдануы және өмірлік маңызы бар ақпараттардың бүтіндігіне зақым келуі болып табылатын АҚШ пен одақтас елдердің Internet-қорларына рұқсат етілмеген енулер.

Талдаудың нәтижесіндегі басты қорытындылар:

- физикалық шабуылдар тез арада желілік шабуылдардың санының өсуіне әкеліп соқтырады;

- желілік шабуылдардың саны, күрделілігі және координациялануы үздіксіз артып отырады;

- желілік шабуылдар өзінің құрамына Internet-ке қосылған серверлер және белсенді желілік құрылғылар кіретін аса маңызды желілік қорларға бағытталған.

Жүргізілген зерттеу лаңкестікпен соғыс кезіндегі қауіпсіздікті қамтамасыз ететін, бірінші орындағы шаралар ретінде келесілерді ұсынуға рұқсат берді:

- құжаттандыру (logging) деңгейін арттыру және желілік шабуылдарды анықтау жүйесіндегі хабарлаулар (alert);

- тексеру жүргізу және сақтық шараларын қабылдау мақсатымен күдікті белсенділерді тез арада құқық қорғау органдарына хабарлау;

- ақпараттық және физикалық қауіпсіздікті қамтамасыз ету облысында стандарттарды ұстану және басты тәжірибені енгізу, АҚ уақытымен жаңартып тұру, вирустардан қорғану, шабуылдарды анықтау жүйесін орнату және ЖЭ;

- шабуылды іске асыратын (exploites) атақты программалық құралдарға қарсы ұсынылған қорғаныс шараларын қабылдау және маңызды ақпараттық қорлардың қосымша (резервті) көшірмесін жасау;

- маршрутизаторлар мен DoS-шабуылдардан қорғану үшін ЖЭ-да IP-пакеттерді іріктеу шараларын қолдану.

Келтірілген ұсыныстардан көрініп тұрғандай, оларсыз автоматтандырылған жүйенің (ЖЭ, қосымша көшірме жасау жүйесі және вирусқа қарсы құралдар секілді) қалыпты жұмыс жасауы мүмкін емес, стандартты қорғаныс құралдары бар жүйеге желілік шабуылдармен күресудің басты құралы IDS-те (шабуылдарды анықтау жүйесі) аса қажет.

Қазіргі таңда IDS бірлескен желілердің қауіпсіздігін қамтамасыз ету тәжірибесіне кең көлемде ене бастады. Бірақ өздерінде шабуылды анықтау жүйесін дамытатын ұйымдар міндетті түрде соқтығатын қиын жағдай-

лар тізімі бар. Бұл жағдайлар аса қиындатады, кейде IDS-тің ену үрдісін тоқтатып та тастайды. Олардың кейбіреулерін келтірейік:

- коммерциялық IDS-терінің қымбат тұруы;
- өтірік іске қосылатын және қосылмайтындардың санының көптігімен дәлелденетін (false positives and false negatives) қазіргі IDS-тердің аз тиімділігі;
- қорларға қойылатын талаптардың қатаң қадағалануы және кейде IDS-тің желіде 100 Мбит/с жылдамдықта қанағаттандырмайтын өнімділігі;
- желілік шабуылдармен байланысты тәуекелдердің қажетті деңгейде бағаланбауы;
- ұйымда басшыларға тәуекелдің көлемін дұрыс бағалауға және оған қарсы шаралардың іске асу құнын есептеуге мүмкіндік беретін тәуекелді талдау және олармен басқару әдістерінің жоқ болуы;
- шабуылдарды анықтайтын жоғары деңгейдегі мамандардың жетіспеуі, ол мамандарсыз IDS-тің бұзып кіруі және дамуы мүмкін емес.

Қазақстанға кәсіпорынның ақпараттық инфрақұрылымының Internetтен аз ғана тәуелділігі және желілік шабуылдарға қарсы тұратын қорғаныстың қымбат түрін иемденуге мүмкіндік туғызбайтын, қалдық принципі бойынша ақпараттық қауіпсіздікті қамтамасыз етіп отырған шараларды қаржыландыру сай.

Оған қарамастан IDS-тің АҚ-ті қолдау тәжірибесіне енуі жалғасып келе жатыр, оған қоса Қазақстанда да.

Американдық институт SANS GIAC Certified Intrusion Analyst (GCIA) шабуылын анықтаумен айналысатын мамандарды кәсіби куәлікпен марапаттау жөніндегі бағдарламаны құптады. GCIA куәлігі маманның тәжірибе жүзіндегі білімінің куәсі бола тұрып АҚШ-та ISC-мен (International Security Consortium) құпталған және АҚ сферасындағы кәсіби кемелділіктің эталоны болып табылатын CISSP-ден (Certified Information Systems Security Professional) де жоғарырақ бағаланады.

Шешім қабылдау барысындағы қателердің, оған қоса желілік шабуылдан қорғаудың негізінде тәуекелді дұрыс бағаламау жатыр. Қызметтің кез келген түрімен байланысты идентификацияның және тәуекелдерді бағалаудың нақтылығы пәндік облыстағы маманның кәсіптік кемелділігінің басты көрсеткіші болып табылады. Тәуекелдің күрделілігі дұрыс бағаланбаса ақпаратты қорғау жүйесін неден бастау, қандай қорлар және қандай қауіптен қорғау және қандай қарсы әрекеттерді күштірек деп санау керектігі жайлы сұраққа жауап беру қиын. Оған қоса қажетті қарсы әрекеттердің қажеттілігі және жеткіліктілігі және олардың тәуекелділікке сай келетіндігі жайлы мәселені шешу де қиын.

Осылайша, желілік шабуылдарға байланысты тәуекелдерді бағалау мәселесі маңызды болып табылады және ол бірінші болып талқыланады.

7.2 Шабуылдарды тәуекелдермен басқару әдісі ретінде анықтау

Шабуылдарды анықтау – бүгінгі таңда тәуекелдермен басқарудың бір әдісі. Желілік IDS-тердің көмегімен желілік шабуылдарды анықтаудың міндеті шабуыл жүргізуші және шабуылданушы желілердің арасындағы желілік трафиктерді бақылау, күдікті трафикті табу және талдау, оның іске асуымен байланысты шабуылдың күрделілік деңгейін бағалау, тәуекелдің маңыздылығы және де шабуылға әсер етуіне байланысты шешімнің қабылдануы болып табылады. Күдікті трафикті іздеу, кейде шабуылдың маңыздылығының деңгейін анықтау да IDS автоматты түрде орындалады. Шабуылдарды анықтаудың ең кең таралған әдісі төменде қарастырылатын және барлық коммерциялық IDS-те қолданылатын сигнатурлы талдау болып табылады. Желілік шабуылмен байланысты тәуекелдің мөлшерін бағалау сарапшының қатысуын талап етеді. Тәуекелді бағалау барысында шабуылға жауап қайтару мәселесі шешіледі. Егер тәуекел мардымсыз болса, онда шабуыл назар аударуға да тұрмайтын болуы мүмкін. Сонда да кейбір жағдайларда шабуылға жылдам қарсы тұру әдістері қажет болуы мүмкін.

SANS/GIAC-мен қабылданған, желілік шабуылдардың іске асуымен байланысты, тәуекелді бағалау әдісін қарастырайық.

7.2.1 Желілік шабуылдың күрделілігін бағалау

Әртүрлі деңгейдегі ауыр тиетін шабуылдар әртүрлі деңгейдегі жауап қайтаруды талап етеді. Шабуылдың ауырлығы (Severity) оның іске асуының нәтижесіндегі тәуекелдің мөлшерімен анықталады. Тәуекелдің мөлшері шабуылдың ойдағыдай жасалуының ықтималдылығынан және мүмкін болатын зиянның мөлшерінен тәуелді, ал мүмкін болатын зиянның мөлшері оған қарсы шабуыл бағытталған қорлардың критикалық дәрежесінен (Criticality) тәуелді. Шабуылдың ойдағыдай жасалу ықтималдылығына (Lethality) оның көмегімен алдын алатын әдістердің тиімділігі және қорғаныс жүйесінің осалдылығының мөлшері әсер етеді. Осалдылық мөлшері қауіптің белгілі бір түріне қарсы тұру үшін қолданылатын, желілік және жүйелік деңгейдегі қарсы әдістердің тиімділігімен тікелей байланысты.

Шабуылдың маңыздылық деңгейін анықтайтын формула келесі түрде болады:

SEVERITY = (CRITICALITY + LETHALITY) - (SYSTEM COUNTERMEASURES + NETWORK COUNTERMEASURES).

Бұл формула IDS-тің көмегімен анықталған, ол шабуылдың кесірінен пайда болған тәуекелдің мөлшерін бағалау үшін қолдануға болады. Көп жағдайда тәуекелдің мөлшері кейбір маңызды мәндерден асып түсетін шабуылдар ғана қызығушылық тудырады.

Шабуылдың маңыздылығының деңгейі (SEVERITY) -10-нан +10 сандық шкаламен белгіленеді.

SEVERITY {-10,10} – желілік шабуылдың іске асуымен байланысты тәуекелдің мөлшері.

Желілік қордың күрделілігі (критичность) (CRITICALITY) берілген желілік қордың міндетінен және олардың қызметтерінен туындаған 5 балдық шкаламен анықталады. Тәжірибеде көбіне келесі шкалаға сүйенеді:

- 5 – ЖЭ, DNS-сервер, бағыттауыш;
- 4 – пошталық көмей;
- 2 – UNIX жұмыс станциясы;
- 1 - MS-DOS, Windows 3.11 дербес компьютерлері.

Шабуылдардың ойдағыдай жасалу ықтималдығын және мүмкін болатын шығынды (LETHALITY) анықтау үшін келесі шкала қабылданған:

- 5 – шабуылдаушы жойылған жүйеде суперқолданушының құқығына ие бола алады;
- 4 – желілік шабуыл іске асқан жағдайда қызмет көрсетуден бас тарту;
- 3 – жойылған жүйеде ешқандай артықшылығы жоқ қолданушының құқығына ие болу, мысалы желіде ашық түрде беріліп жатқан парольді ұстап қалу жолымен;
- 2 - желілік рұқсат етілмеген енудің кесірінен ақпараттың құпиялылығының жойылуы, мысалы Windows жүйелеріне жасалатын null session шабуылдары;
- 1 – қабылданған шабуылдың ойдағыдай болу ықтималдығы өте аз.

Жүйелік деңгейдегі қабылданған қарсы әдістердің тиімділігін (SYSTEM COUNTERMEASURES) келесі шкаламен бағалауға болады:

- 5 – қазіргі заманға сай ОЖ, барлық бағдарламалық түзетулер енгізілген (жаңарту пакеттері), қосымша (орнатылған) желілік қорғаныс жабдықтары бар (мысалы, tcp wrappers немесе secure shell);
- 3 – ОЖ-нің ескірген нұсқасы, кейбір бағдарламалық түзетулер енгізілмеген;
- 1 – арнайы қорғаныс тәсілдері жоқ, парольдермен басқару саясаты ұйымдаспаған, парольдер желі бойымен ашық түрде беріледі.

Келесі шкала желілік деңгейдегі қарсы әдістердің тиімділігін бағалау үшін қажет (NETWORK COUNTERMEASURES):

- 5 – артықшылықтарды минималдау принципін іске асыратын ЖЭ, желіге қосылудың жалғыз нүктесі болып табылады;
- 4 – ЖЭ және желіге қосылудың қосымша нүктелерінің болуы;
- 2 – ашық түрде тыйым салынбағандардың бәріне рұқсат беретін ЖЭ (енумен басқарудың рұқсат ету саясаты).

Белгіленіп кеткендей, желілік шабуылдармен байланысты тәуекелді басқарудың бұл әдісі SANS/GIAC-та, желілік IDS-тердің көмегімен анықталған, желілік трафиктің күдікті бөліктерін талдау барысында қолданылады.

7.3 Желіаралық экранның шектеулері

Қазіргі таңда Internet-тен төнетін қауіптен қорғану үшін дәстүрлі ЖЭ-ның жеткіліксіз екені анық байқалады, себебі олар толық бір қауіпсіздік қаупінен қорғанысты қамтамасыз ете алмайды (оған қоса ЖЭ-ның өзіне төнген кауіптен де). ЖЭ-ны қосқанда, ақпаратты қорғаудың дәстүрлі әдістері тек белгілі осалдықтарға ғана қарсы қолдануға тиімді. Олар хакерлерге шабуыл жасаудың жаңа әдісін табуға кедергі жасай алмайды. Бұл үшін шабуылдарды анықтаудың арнайы түрі ұсынылған, ол – IDS. Оған қоса, ЖЭ-ны орнату бірлескен жүйенің Internet тарапынан төнетін қауіптен қорғаныс деңгейін төмендететін жағдайлар өте көп. Дұрыс орнатылмаған ЖЭ қорғаныс жүйесінде кейде оның болмағанынан да үлкен «саңылау» туғызады.

Көліктің қауіпсіздік деңгейін арттыруға арналған, барлық таксилерді құлыптуға қарсы (антиблокировка) тежегішпен (ABS) жабдықтау жөніндегі американдық тәжірибемен ұқсастығы бар. Статистика бойынша таксисттердің қатысуымен болған жол апаты бұл тәжірибенің нәтижесінде артып кетті, себебі жүргізушілер тежегішке көп сеніп, жолда қауіпті жүре бастады. Осылайша, ABS, қауіпсіздік деңгейін, жүргізуші көлікті бұрынғыша айдаған жағдайда ғана арттыратын болып шықты.

Дәл сол ұстаным ЖЭ-ға және басқа кез келген қорғаныс тәсілдеріне әділ болып табылады.

Желіге жаңа қорғаныс тәсілін қосу жүйенің жалпы қорғанысын, тек қазіргі уақыттағы қауіпсіздікті қамтамасыз ету тәжірибесі қорғаныс механизмінің нашарлауына әкеліп соқтырмайды деген шартпен ғана арттырады.

ЖЭ-ны орната отырып, желілік администраторлар іске асатын ЖЭ-ға сене отырып қорғаныс механизмдері, ЖЭ жоқ болған жағдайда қажет болатын, сыртқы желіден келетін қауіптен қорғануды қолдау жөніндегі қосымша іс-шаралардан жиі бас тартып отырады. Нәтижесінде желінің сыртқы шабуылдардан жалпы қорғанысы артып немесе өзгеріссіз қалып, немесе (және бұл ең ықтималды жағдай) төмендеуі мүмкін. Бұл администраторлар мен желінің қолданушылары ЖЭ-ға толығымен сенгендіктен және желінің Internet тарапынан келетін сыртқы қауіптерден қорғаныс барысында оның рөлін асыра бағалағандықтан болады. Олар ЖЭ жаңбырдан, бұршақтан, қардан, теңіз дауылынан және басқа да көптеген қолайсыз ауа райынан қорғайтын қалқан ретінде елестетеді. Солай бола тұра олар, қалқанда біраз саңылаулар болатынын, кейде ол тіпті тор секілді болатынын ұмытып кетеді. Қалқандағы «саңылаулар» сыртқы қарсылас әлеммен араласу үшін керек. Қателесіп, кейде қажет емес «саңылаулар» ашық қалуы немесе ол «саңылаулар» тым үлкен болуы мүмкін, оған қоса қалқандағы «саңылауларды» кейде сыртынан бұзып кетуі де мүмкін.

Осылайша, ЖЭ-ға жоғары деңгейдегі қорғанысты қамтамасыз ету үшін шабуылдарды анықтауды міндетті түрде арнайы тәсілдермен толықтырып отыру қажет. Бұл тақырыпқа қазірдің өзінде жеткілікті құлақтандырулар бар, сондықтан бұл тезисті ресейдің және шет елдік серіктестіктердің қайғылы тәжірибесінен алынған көптеген мысалдармен толықтырып, қайтадан дәлелдеп шығудың қажеті жоқ. Бірақ, ЖЭ-ны орната отырып, ресейлік серіктестіктердің басқармалары шабуылдарды анықтайтын жүйені иемденуге және оларды пайдалануға, ұсынуға қаражат бөлуге асығар емес.

7.4 Күдікті трафикті талдау

7.4.1 Сигнатуралар шабуылдарды анықтайтын басты механизм ретінде

IDS шабуылдарды анықтау жүйесі ақпараттық жүйені, қауіпсіздікті бұзу және оларға жедел жауап қайтару мақсатымен желілік, жүйелік және қолданбалы деңгейде бақылау мәселесін шешеді. Желілік IDS-тер желілік пакеттерді талдауға қажетті деректер көзінің рөлін атқарады, ал жүйелік деңгейдегі IDS (хосттық - host based) ОЖ-нің және қосымшалардың қауіпсіздігін тексеретін журналдардың жазбаларын талдайды. Оған қарамастан, талдау әдістері (шабуылдарды анықтау) IDS-тің барлық кластары үшін ортақ болып қала береді.

Шабуылдарды анықтау мәселесін шешуге көптеген әртүрлі жолдар ұсынылды (жалпы жағдайда құрамына шабуылдардан басқа берілген өкілеттіліктің төңірегінде орындалатын іс-әрекеттер кіретін, бірақ қауіпсіздік саясатының қалыптасқан ережелерін бұзатын, қасақана жасалған белсенділік туралы айтылып отыр). Бірақ әлі де бар IDS-терді екі басты кластарға бөлуге болады: біреулері – статистикалық талдауды, басқалары – сигнатуралы талдауды қолданады.

Статистикалық әдістер, қаскүнемнің белсенділігі әрқашан әлдебір ауытқуларға, қолданушылардың, программалардың және аппаратуралардың мінез-құлқының көрінісінің өзгерісіне байланысты өзгеріп отыруы жайындағы болжамдарға негізделеді.

Көптеген жаңа коммерсиялық өнімдермен қабылданған, шабуылды анықтаудың негізгі тәсілі - сигнатуралық талдау болып табылады. Берілген тәсілдің салыстырмалы түрдегі қарапайымдылығы оны тәжірибеде сәтті қолдануға мүмкіндік береді. Сигнатуралық талдауды қолданатын IDS, әдетте, ЖЭ-ны іске қосатын қауіпсіздік саясатының ережелері туралы ешнәрсе білмейді (сол себепті осы жағдайда алдын ала ойластырылған белсенділік жайында емес, тек шабуылдар жайында айтылады). Оларды функциялаудың негізгі принципі – желі/жүйеде болып жатқан оқиғаларды атақты шабуылдардың сигнатураларымен салыстыру – антивирустық АҚ-да қолданылатын сияқты.

Ақпараттық технологияның (ISO 15408) қауіпсіздігін бағалаудың жалпы белгілері «Қауіпсіздік аудит мәліметтерінің талдауы» (Security audit analysis) атты FAU_SAA талаптар жинағын құрайды. Бұл талаптар IDS-тің функционалдығын анықтайды, олар қаскүнемді статистикалық және сигнатуралық талдау әдістерімен іздейді.

FAU_SAA2 «Профильді қолдануға негізделген тосыннан болған белсенділікті айқындау» (Profile based anomaly detection) компоненті жүйенің профильдерінің көмегімен тосыннан болған белсенділікті анықтауды жорамалдайды, олар жүйенің қолданушыларының әрекетінің қауіпсіздігінің көзқарасымен алғанда қауіпті болып табылады және сол әрекеттерді айқындайды. Кез келген қолданушының әрекетінің қауіпсіздік деңгейін орнату мақсатында әрбір қолданушыға сәйкес келетін «сенімсіздік рейтингі» есептеледі. Қолданушының әрекеті қауіпті болған сайын, оның «сенімсіздік рейтингі» жоғары болады. «Сенімсіздік рейтингі» белгіленген критикалық мәнге жеткен кезде, қауіпсіздік саясатымен алдын ала қарастырылған, қаскүнемдік белсенділікке әсері бар әрекеттер іске асады.

FAU_SAA3 «Шабуылдың қарапайым эвристикасы» (Simple attack heuristics) және FAU_SAA4 «Шабуылдың күрделі эвристикасы» (Complex attack heuristics) компоненттері қаскүнемді белсенділікті анықтауға қажетті сигнатуралы талдауды орындауды қарастырады. FAU_SAA4 шабуылы болған жағдайда сигнатура оқиғалар жүйелілігін ұсынады, бұл қауіпсіздік саясаты жүйесіндегі орнатылған ережелерді бұзу белгісі болып табылады.

7.4.2 Желілік трафикті талдау және контенттік талдау

Желілік шабуылдарды анықтайтын бір-бірін тежемейтін екі жолы бар: желілік трафикті талдау және контенттік талдау. Бірінші жағдайда тек желілік пакеттердің тақырыптары ғана зерттеледі, ал екіншісінде – оның құрамы зерттеледі.

Әрине, ақпараттық өзара әрекеттесуді толық қадағалау тек жүйелі пакеттердің құрамын, оның тақырыптары мен мәліметтер аймағын қоса алғанда толығымен талдау жолымен ғана қамтамасыз етіледі. Дегенмен, тәжірибе көрсеткендей, мұндай тапсырманы орындау қиын, себебі өңдеуді қажет ететін мәліметтер қорының көлемі үлкен. Қазіргі заманғы IDS желіде 100 Мб/с жылдамдық кезінде де өндірушілік жағынан үлкен қиындықтарға ұшырай бастады. Сондықтан көп жағдайларда шабуылдарды анықтау үшін желілік трафиктің талдауына, кейбір жағдайларда оны контенттік талдаумен біріктіре отырып жүгіну мақсатқа лайықты.

Тұжырым бойынша желілік шабуылдың сигнатурасының вирус сигнатурасынан еш айырмашылығы жоқ. Ол өз кезегінде белгілер жиыны болып табылады, олар желілік шабуылдарды желілік трафиктің басқа түрлерінен айыруға мүмкіндік береді. Сонымен, төменде келтірілген белгілер шабуылдар сигнатурасы ретінде қарастырыла алады:

- трафикті талдау кезінде қолданылатын шабуылдар сигнатурасының мысалдары (желілік пакеттердің тақырыптары):

- TCP-пакет тақырыбында 139 тағайындау порты және OOB (Out of Band) жалаушасы орнатылған, бұлар WinNuke үшін шабуыл жасалу белгісі болып табылады;

- TCP-пакетінің бір мезгілде, бір-біріне қарсы келетін тулары орнатылған: SYN және FIN. Тулардың берілген комбинациясы арқылы көптеген шабуылдайтын программаларда тек жекелік SYN-жалаушасының орнатылуын тексере алатын сүзгілер мен мониторларды айналып өтуге болады;

- контентаны талдау кезінде қолданылатын шабуылдар сигнатурасының мысалдары: GET. cgi-bin/etc/passwd". HTTP-пакетінің мәліметтер аймағында мұндай қатарлардың пайда болуы phf, php немесе aglimpse типтегі эксплойттардың бар екендігін дәлелдейді.

Контентті талдау әдістерінің тағы да бір кемшілігі бар. Шабуылдаушы программалар (DDoS, trojans) трафикті шифрлеуге назар аударған кезде, олар жұмыс істемейді. Мысалы, Back Orifice trojan немесе Barbwire DDoS-та клиент пен сервердің (менеджер және агент) арасында жіберілетін бұйрықтар blowfish алгоритмі арқылы шифрленеді. Шабуылдардың мұндай түрін анықтау тәсілі желілік пакеттердің тақырыптарын талдаумен шектеледі.

7.4 IDS тәуекелмен басқару құралы ретінде

7.4.1 Шабуылдарды анықтау жүйесінің типтік архитектурасы

Шабуылды анықтау жүйесінің типтік архитектурасы, ереже бойынша, келесі компоненттерді құрайды:

- сенсор (ақпаратты жинау құралы);
- анализатор (ақпаратты талдау құралы);
- әсерлесу құралы;
- басқару құралы.

Әрине, бұл барлық құрамдас бөліктер бір компьютерде және тіпті бір қосымша шекарасында жұмыс істей алады, дегенмен көп жағдайда олар шекарасына және атқаратын қызметіне байланысты үлестірілген. IDS-тің мұндай құрамдас бөліктері, анализаторлар және басқару құралы ретінде, сыртқы желідегі ЖЭ-ның артына орналастыру қауіпті, себебі егер олардың осал жерлері байқалып қалса, онда қаскүнем IDS-пен қолданылатын, ережелер базасын талдау негізінде ішкі қорғалатын желінің құрылымы туралы ақпарат ала алады.

Шабуылды анықтау жүйесінің типтік архитектурасы 7.1-суретте бейнеленген. Желілік сенсорлар желілік трафикті ұстап қалады, хосттық сенсорлар үшін ақпараттар көзі ретінде ОЖ, мәліметтер қорымен басқару жүйесі (СУБД) және қосымшалардың оқиғаларын тіркеу журналдары қол-

данылады. Оқиғалар туралы ақпараттарды тікелей ОЖ ядросынан, ЖЭ-дан және қосымшалардан хосттық сенсор арқылы алуға болады. Қауіпсіздік серверінде орналасқан анализатор, сенсордан түсетін ақпаратты талдайды және оларға орталықтандырылған жиын жүргізеді.

Әсер ету құралдары желіні бақылау станцияларында, ЖЭ-да, серверлерде және ЖЕЖ жұмыс станцияларында орналасуы мүмкін. Шабуылдарға әсер етуі бойынша қарапайым іс-әрекеттердің жинағының құрамына қауіпсіздік администраторын хабарлау (электрондық пошта арқылы, хабарламаның консольге шығуы немесе пейджерге жіберу), желілік сессияларды және тіркелетін қолданушылар жазбаларын шабуылдарды тез арада тоқтату мақсатымен құлыпқа қою, сонымен қатар шабуылдаушы тараптың әрекеттерін хаттамалау кіреді.

Басқару құралдары шабуылдарды анықтау жүйесінің барлық құрамдас бөліктерін администрациялауға, қауіпсіздікті бұзуды анықтайтын алгоритмдерді құруға және оларға әсер етуге (қауіпсіздік саясаты) арналған, сонымен қатар, бұзулар мен есеп беру генерациясы жайындағы ақпаратты көруге арналған.

7.1-сурет. Шабуылдарды анықтау жүйесінің типтік архитектурасы

7.4.2 Шабуылды анықтау жүйесінің компоненттерінің арасындағы өзара әрекеттесу ережелерін анықтайтын стандарттар

IDS-те қолданылатын, мәліметтермен алмасу хаттамаларын және мәліметтердің форматтарын стандарттау қажеттілігі төменде келтірілген себептермен түсіндіріледі. Internet желісіне қосылған жергілікті есептеу желінсін (ЖЕЖ) үлестірілген координацияланған шабуылдардан қорғау

үшін, ЖЕЖ-ге әртүрлі кіріс нүктелерін қорғауға арналған, IDS-тер арасындағы өзара әрекеттесудің белгілі бір деңгейін қамтамасыз ету қажет. Мысалы, бір ЖЕЖ-ге қарсы шабуыл жасалған жағдайда, шабуыл көзінің IP- мекен-жайын құлыптау жолымен ЖЭ кескінінің өзгерісі қарастыратын әсер ету ережесі, сондай өзгерістер қалған ЖЭ-ны қорғауға арналған барлық ЖЭ-да болуы қажет. Бұл үшін шабуыл көзі және әртүрлі IDS-тер арасындағы әсер ету әдісі жайында ақпарат ауысуы қажет.

IDS-тің орталық құрамдас бөлігі анализатор (analysis engine) болып табылады, яғни, сенсорлардан келіп түсетін мамандандырылған программалық ядро және күдікті әрекеттерге әсер ету әдістері жайында шешім қабылдау. Анализаторлардың арасындағы мәліметтермен алмасу форматы мен хаттамаларды стандарттау, бір жағынан, сенсорлармен және әсер ету құралдарымен, екінші жағынан, әсер ету құралдары мен сенсорлардың әртүрлі типтеріндегі анализатордың жалпы программалық ядросын қолдануға мүмкіндік береді.

IDS–те қолданылатын мәліметтермен алмасу форматы мен хаттамаларды стандарттау баяғыда басталды. Бірнеше атақты мәліметтер форматын қарастырайық, олардың көмегімен Internet арқылы қауіпсіздіктің бұзылғандығы жайлы ақпаратпен алмасады.

7.4.3 Мәліметтермен алмасу форматы

AusCERT (portmap probe)

Source: 210.177.64.1
Ports: tcp 111
Incident type: network scan
re-distribute: yes
timezone: GMT + 1300
reply: no
Date: 30th Jan 2000 at 22:01 (UTC)

AusCERT жүйесі шабуылдар жайында статистикалық ақпаратты талдау және жинау үшін қолданылады. Жазбаның берілген форматы AusCERT мәліметтер қорына шабуылдар туралы ақпаратты автоматты түрде қосуға мүмкіндік береді.

Граифиннің тізімдері (Griffin list). Графин тізімдерінің көмегімен ойын-сауық орталықтарында карточкалық алдаушыларды табады. Атақты алдаушылардың суреттері бар файлдар бейнетаспалардан алынған кескіндермен салыстырылады. Ұқсас белгілері ретінде уақыт өтуіне байланысты өзгермеген бет әлпеттер қарастырылады.

Шабуылдарды анықтау жүйесінде орнатылған Графин тізімдерінің құрамына күдікті іс-әрекеттер жиі жасалатын, компьютерлердің желілік мекен-жайлары кіреді. CERT немесе GIAC тәрізді компьютерлік оқиғаларға әсер етуі жөніндегі Internet-орталықтар, осындай тізімдерді құрумен

және кең жұртшылыққа оларға рұқсат алып берумен айналысады (www.incidents.org). Бұл мәліметтер IDS-те қолданыла алады. Күдікті трафикті талдау кезінде ерекше назарды өз беделін жоғалтқан IP мекен-жайларға аудару қажет.

7.4.4 CVE – осалдылық тезаурусы

CVE (Common Vulnerabilities and Exposures) – бұл барлық атақты осалдылықтардың бірыңғай тезаурусы, ол барлық қызығатын тұлғалар үшін оған Internet арқылы рұқсат ала алатын, олардың аталуының жалпы ережелерін анықтайды (cve.mitre.org). CVE осалдылықтарды топтастырушы болып табылмайды және олардың жүйеленуіне үміттенбейді. Оның пайда болуының тарихына қысқаша тоқталып кетейік.

Американдық MITRE бірлестігінен шыққан Дэвид Манн (David Mann) және Стивен Кристи (Steven Christey) осалдылық мәліметтер қорын құру жолында біраз жұмыс атқарды. Осалдылықтар арасында ұқсастық орнату қажет болды, олар хабарламалармен және осы осалдылықтарды жою туралы ұсыныстармен ескертілетін, әртүрлі қорғау сканерлерінің көмегімен табылады. Осы жерде олар осалдылықтарға ат беру мәселесіне келіп тірелді. Мысалы, атақты CGI phi осалдылығы SHELL бұйрықтық түсініктемелердің метасимволдарын қолдану арқылы жойылған түрде бұйрықтарды орындауға мүмкіндік береді. Осы осалдылықтың көмегімен cat/etc/passwd бұйрығын орындау арқылы паролі бар файлды алу мысалы классикалық болып табылады. CERIAS хабарламаларында бұл осалдылық httpd_escshellcmd деп аталады, ал CERT хабарламаларында – CA-96-06.CGI_Example_code деп аталады. Түрлі желілік сканерлерде, мысалы Internet Scanner және CyberCop Scanner-де, осалдылыққа ат берудің әртүрлі әдістері қолданылады.

Ақпараттық ресурстардың осалдылықтарын классификациялаудың проблемаларын зерттеу, Дэвид Манн мен Стивен Кристи екеуіне соның төңірегінде осалдылықтарға біртекті ат беру жөніндегі тұжырымдама құрылған, CERIAS-та өткізілетін, бірқатар жұмыстарды жасауға мүмкіндік берді. Бұл тұжырымдама Towards a Shareable Vulnerability Database есеп беруінде құрылды, ол 1999 жылы CERIAS-пен өткізген CERIAS Workshop for Vulnerability Databases мәслихатында таныстырылды.

CVE түрлі желілік сканерлердің мүмкіндіктерін салыстыру тапсырмасын мейлінше жеңілдетеді. CVE-бірлескен сканерлері үшін табылатын осалдылықтардың тізімін өзара қатар орналастыру жеткілікті. Егер де сканерлер осалдылықты атау үшін әртүрлі мән білдіретін жүйелерді қолданса, онда оларды салыстырудың ешбір мәні болмайды.

Қазіргі уақытта Symantec, NAI, ISS, Cisco және т.б. қоса желілік сканерлерді және басқа да қорғанысты бақылау тәсілдерін құрушылардың

көпшілігі өз өнімдеріне ат беруде, стандартты әдісі ретінде, CVE-ні қолдайтындары жөнінде хабарлады.

7.4.5 CIDF

CIDF (Common Intrusion Detection Framework) шабуылды анықтау жүйесінің біртекті архитектурасы ынталандыратын болып табылады, осыған сәйкес желілік хаттамалар мен IDS құрамдас бөліктерінің өзара әрекеттесуіне арналған, қолданбалы программалау интерфейсі ойлап табылған.

CIDF келесілерді анықтайды:

- осалдылықтар, оқиғалар, оқиғаларға әсер ету әдістері және шабуылдар жайындағы ақпараттармен таныстыруға арналған мәліметтер модулі;
- IDS компоненттерінің өзара әрекеттесу модулін;
- IDS компоненттерінің өзара әрекеттесуінің хаттамалары мен интерфейстері.

CIDF моделінде шабуылдар мен осалдылықтар S-белгісінің көмегімен сипатталады. Теорияға тоқталмай-ақ, мұның не екенін түсіну үшін, файлды жоюмен байланысты оқиғаға арналған S-белгісіне мысал келтіреміз (листинг 2-ні қараңыз).

Листинг 2

```
Delete
(Context
(HostName ’first.example.com’)
(Time ’16:40:32 Jun 14 1998’)
)
(Initiator
(UserName ’lp’)
)
(Source
(FileName ’/etc/passwd’)
)
)
```

Берілген S-белгісі lp қолданушысы 1998 жылы 14 маусымда 16:40:32 кезде first.example.com компьютерінде /etc/passwd файлын өшіргеніне негізделген оқиғаға арналған.

Қазіргі уақытта CIDF статусы анықталмаған, дегенмен ол ID саласындағы стандарттарды өңдеуге арналған тұжырым базасы болып қала бермейді және IDWG стандартын құру барысында негіз ретінде алынуы мүмкін.

7.4.6 IDWG жұмыс тобы

IDWG (Intrusion Detection Working Group) шабуылдарды айқындау саласындағы Internet-стандарттарын құруға арналып жасалған IETF жұ-

мысшы тобы болып табылады. IDWG мәліметтердің және өзара әрекеттесетін хаттамалардың жалпы форматын құру және IDS-тің әртүрлі компоненттері арасындағы ақпаратпен алмасу тапсырмасын шешеді.

IDWG жұмысшы тобын құру кезінде олардың қатысушыларының алдында келесі тапсырмалар тұрды:

- шабуылды айқындау жүйелері IDS пен желілі басқару құралдарының арасындағы, өзара әрекеттесу ережелерін ұсынатын, жоғарғы деңгейдегі функционалды талаптарының негізделген таңдауы;

- осы талаптарға сай және IDS-тер арасындағы мәліметтермен алмасу форматын орнататын, IDS-тің өзара әрекеттесуінің ортақ тілінің егжей-тегжейі;

- IDS-тер арасындағы өзара әрекеттесудің хаттамаларын сипаттайтын және осы хаттамаларда мәліметтермен алмасудың ортақ форматының қолданылуына мүмкіндік беруі жөніндегі құжаттарды толтыру.

Қазіргі уақытта IETF IDWG жұмысшы тобының күшімен IDS-тер арасындағы мәліметтермен алмасуының хаттамалары мен форматтарына арналған басты Internet стандарттарын жасау жұмысы аяқталды.

IDWG-мен ұсынылған Internet желісінің стандарттарының бар жобалары:

- Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition;

- The TUNNEL Profile;

- The Intrusion Detection Exchange Protocol (IDXP).

IDMEF (Intrusion Detection Message Exchange Format) – IDS құрамдас бөліктері арасындағы мәліметтермен алмасу форматы. Ол шабуылды анықтау жүйелері арасындағы күдікті оқиғалар жайында ескертетін хабарламаларды жіберумен айналысады. Бұл формат коммерциялық және еркін таралатын IDS-тер арасындағы ұқсастықты және қорғаныстың жоғарғы деңгейін қамтамасыз ету үшін қажетті өзара әрекеттесуді қамтамасыз етуі қажет.

IDMEF мәліметтер модулі XML DTD түрінде сипатталады.

Желілік сенсор/талдаудың ping of death шабуылы жайындағы хабарламасы 3-листингте көрсетілген. Шабуылдың бірнеше объектілері бар. Шабуылдаушының IP мекен-жайы жасанды болып табылады.

3-листинг

```
<?xml version="1.0" encoding="UTF-8"?>
sensor.bigcompany.com
2000-03-09T10:01:25.93464Z
222.121.111.112
123.234.231.121
lollipop
Cabinet B10
```

Cisco.router.b10
CVE-1999-128
http://www.cve.mitre.org/

IDMEF (<portlist> белгісі сканирленетін порттардың нөмірін білдіреді) форматында көрсетілген желілік сенсордың/анализатордың портты сканирленгендігі жөніндегі хабарлама 4-листингте кескінделген.

4-листинг

<?xml version="1.0" encoding="UTF-8"?>
Headquarters Web Server
analyzer62.bigcompany.com
2000-03-09T15:31:00-08:00
222.121.111.112
www.bigcompany.com
123.234.231.121
5-25,37,42,43,53,69-119,123-514

IAP (Intrusion Alert Protocol) – қолданбалы деңгейдің хаттамасы, ол шабуылды анықтау жүйесінің құрамдас бөліктеріне жасалған шабуылдар (alerts) жөніндегі хабарламалармен алмасуға мүмкіндік береді: араларында proxy-сервисі (P) және көмейі болуы мүмкін (G) сенсор/анализатор (S) және менеджерлер (M) арасындағы. Хаттама мәліметтердің көрсетілген форматына тәуелді емес.

7.5 Коммерциялық IDS-тердің мүмкіндіктері

7.5.1 Symantec компаниясының ақпараттарын қорғау құралдары

Symantec компаниясы қазіргі уақытта ақпаратты қорғаудың программалық құралын шығарушылардың арасындағы ірілердің қатарына кіреді және и IBM, CA, ISS, Cisco Systems, Check Point сияқты басқа да компаниялармен салыстырғанда нарықта жетекші орын алады. Symantec компаниясымен болжанатын программалық өнімдер базадағы бірлескен желінің қорғаныс жүйесін құруға мүмкіндік береді, олар бір шығарушының өзінің аспапты құралдары арасында интеграцияланады. Symantec ақпаратты қорғаудың программалық құралы бірлескен клиенттерге негізделген және аппаратты-программалық өнімдердің келесі кластарын көрсетеді:

- желі аралық экран және VPN құралдары (Symantec Enterprise Firewall/VPN);
- қорғанысты бақылаудың құралдары (Symantec Enterprise Security Manager (ESM), Symantec NetRecon);
- шабуылды және тосын құбылысты анықтау жүйесі (Symantec Intruder Alert, Symantec ManHunt);
- антивирустық жабдықтар және контентті талдау құралдары (Symantec AntiVirus, Symantec Web Security);

- орталықтандырылған басқару құралы (Symantec Gateway Security, Symantec Client Security);

- Администрациялау құралы (Symantec pcAnywhere, Symantec Ghost) және т.б.

Symantec компаниясының өнімдері кез келген қиындық деңгейі үшін бірлескен желіні қорғау үшін шабуылды анықтаудың комплексті жүйесін құруға мүмкіндік береді. Функционалды мүмкіндіктердің сипаттамасын бұзбай-ақ, қазіргі кездегі коммерциялық IDS мысалы ретінде Symantec Intruder Alert программалық өнімін қарастырамыз.

7.5.2 Symantec Intruder Alert

Symantec Intruder Alert (ITA) программалық өнімі (host-based) жүйелік деңгейдегі IDS-тің лайықты өкілі болып табылады, ол интеллектуалды программалық агенттер технологиясымен құрылған. Ауқымды және жойылатын шабуылдарды анықтау жүйелі және қолданбалы АҚ оқиғаларын тіркеу журналын талдау жолымен іске асырылады. Осы жүйенің тиімді тұстары – иілгіштігі, ауқымдылығы және администрациялау қарапайымдылығы. ITA қосымшаның кез келген түрімен оңай интеграциялана алады.

Шабуылдарды анықтау және оларға әсер ету нақты уақытта өтеді, оған қоса шабуылдарға автоматы түрде жауап қайтаруы бойынша әрекеттің 14-нұсқасы қарастырылған.

Алдын ала анықталған қауіпсіздік саясатының мәнді мөлшері программалаусыз өзіндік саясаттың құру мүмкіндігімен үйлеседі.

ITA құрамына Windows және NetWare, UNIX ОЖ-сін қосқанда, 35 әртүрлі программа – аппараттық платформаларға арналған программалық агенттер кіреді. Платформаны қамту алаңының көлемінің үлкендігі жағынан бұл өнімге тең келетіні жоқ.

ITA үлестірілген агент/менеджер/консоль үшкомпонентті архитектурада құрылған. ITA-ның барлық компоненттері қорғалған клиент-сервер хаттамасы бойынша өзара әрекеттеседі. Компоненттер арасындағы аутентификация және сеанстық кілттерді өндіру Диффи-Хелман алгоритмі бойынша орындалады. Байланыс сеансын қорғау 400-биттік кілттермен шифрлеу алгоритмі негізінде іске асырылады.

ITA басқару құралдары екі графикалық қосымшамен көрсетілген: ITA Admin және ITA View.

ITA Admin қосымшасы жүйенің компоненттерін басқару үшін, қауіпсіздік саясатын баптау және құру үшін арналған, олар күдікті белсенділікті және оған әсерді айқындау ережесін анықтайды. ITA Admin қосымшасының көмегімен қауіпсіздік администраторы шабуылдарды анықтау жүйесін администрациялау бойынша келесі әрекеттер жинағын көрсете алады:

- агенттерді домендерге біріктіру;

- қауіпсіздік саясатын қалыптастыру және оларды бақыланатын домендерде қолдану;

- Symantec компаниясының Web-серверінен жаңа қауіпсіздік саясаттарын жүктеу;

- экспорт файлдарына қауіпсіздік саясатын экспорттау;

- программалық агенттердің параметрлерін баптау;

- программалық агенттердің көмегімен талдау жүргізу үшін қосымша мәліметтер көзін іске қосу;

- ITA-дің қолданушыларының жеңілдіктерін анықтау және администрациялық рөлдерді шабуылдарды анықтау жүйесін басқару бойынша орналастыру.

ITA View шабуылдар жайында және басқа да күдікті оқиғалар жайында тіркейтін ақпаратты қарастыру құралы болып табылады, олар қауіпсіздік саясаты ережелерімен орнатылғандарға сәйкес ITA агентімен тіркеледі. Бұл құрал ITA мәліметтер қорына өтініштер құруға мүмкіндік береді, олардың құрамына барлық бақыланатын жүйелер жайындағы нақты мәліметтер кіреді, сонымен қатар түрлі графикалық форматта берілген сұраныстың нәтижесінің негізінде есеп беруді құрастыру.

Шабуылды анықтайтын жүйенің орталықтандырылған компоненті ITA Manager болып табылады. Ол бақыланатын объектілердің күйлері туралы ақпаратты ала отырып, оған қосылатын агенттерді реттеумен айналысады, домендер тізімін және оларға белсенді болатын қауіпсіздік саясатын қолдап отырады және қауіпсіздіктің мәліметтер қорымен басқарады. Қауіпсіздіктің мәліметтер қорында тексерілетін объектілердегі қауіпсіздіктің бұзылуы жайындағы мәліметтер бар.

UNIX ОЖ-де ITA Manager қосымшасы «демон» түрінде іске асқан, ол ОЖ Windows NT-да қызметі және ОЖ NetWare-да NLM-модулі болып табылады.

ITA Agent шабуылдарды анықтау жүйесінің "жұмысшы жылқысы" болып табылады, ол бір мезгілде шабуылдарға әсер беру құралы, анализатор, сенсор қызметтерін атқарады. Оның қызметіне ITA қауіпсіздік саясатының ережелері бойынша берілетін, шабуыл сигнатураларын қолданумен әртүрлі қайнар көздердің қауіпсіздік аудитінің мәліметтерін талдау және жинау кіреді. Шығыс мәліметтердің құрамынан шабуыл сигнатурасын анықтаған жағдайда, сәйкес ережелермен ұйғарылған іс-әрекеттер жиыны іске асады.

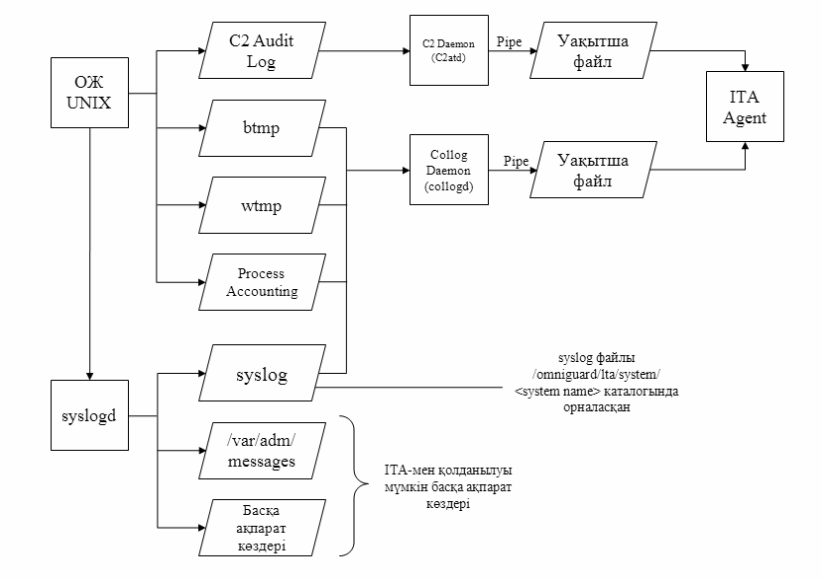
Шабуылдарды айқындау және оларға әсер ету арнайы алгоритм бойынша уақыттың нақты масшабында іске асады (қауіпсіздік саясатының ITA терминологиясында). UNIX ОЖ ортасында агенттер «демондар» түрінде іске асқан, ал Windows NT ОЖ–да қызмет түрінде, ал NetWare-де NLM-модульдерін құрайды. Әр қолдалатын ОЖ үшін ақпаратының аудитінің өзіндік қайнар көзі айқындалады. UNIX және Windows жүйелерінде

қауіпсіздікпен байланысты оқиғалар, жүйелі оқиғалар тіркемесінің стандарты құралдарымен және қауіпсіздік аудитінің құралдарымен тіркеледі (syslog, wtmp, process accounting, btmp, жүйе ішіндегі C2 және с.с. UNIX ОЖ-де жүйелі журнал, қосымшалар журналы және қауіпсіздік журналы Windows NT ОЖ). Сенсорлы модульдер ITA Agent анықталған периодтылығымен жүйелі журнал және аудит журналдарының файлдарын сканерлейді, аудит мәліметтерін санайды және олардың ішкі форматын өзгертеді. NetWare-да ITA Agent сенсорлы модульдері өздігінен тіркейді және бұл ақпаратты ОЖ ядросынан тікелей ала отырып, оқиғалар жайындағы мәліметтерді өңдейді.

UNIX ортасында жүйенің күйі жайында ақпаратты жинау процесі 7.2-суретте көрсетілген. Intruder Alert келесі ақпараттар көзіне автоматты түрде мониторинг жүргізеді:

- құрамында ОЖ ядросынан алынған мәліметтер және syslog жүйесі арқылы тіркелетін қосымшалары бар syslog файлына;
- құрамына жүйеде тіркелген қолданушылар туралы ақпарат және олардың көмегімен іске қосылған процестер кіретін wtmp файлына;
- btmp файлына, онда жүйеге кірудің барлық сәтсіз әрекеттері туралы мәліметтер бар;
- pacct қолданушылар процесінің есеп беру жүйелері, олар өздерінің функционалдануымен және жүйелік қорларды қолдануымен байланысты, әртүрлі ақпараттарды тіркейді;
- C2 қауіпсіздік аудит журналдарын (бұл қайнар көзге жүгіну арнайы ITA баптаудан кейін мүмкін, себебі UNIX-тің әртүрлі іске асуларындағы қауіпсіздік аудитінің ішкі жүйесі әртүрлі орнатылған).

Онда мәліметтер екілік жүйеде сақталатын файлдар болып табылатын, келтірілген ақпараттың көздерінен басқа, қосымша ақпараттық қайнар көздер қосылуға болады, олар мәліметтерді сақтаудың мәтіндік форматын қолданады, мысалы /var/adm/messages файлды және қосымшалар мен ОЖ-нің оқиғаларын тіркейтін журналдың мәтіндік файлы.



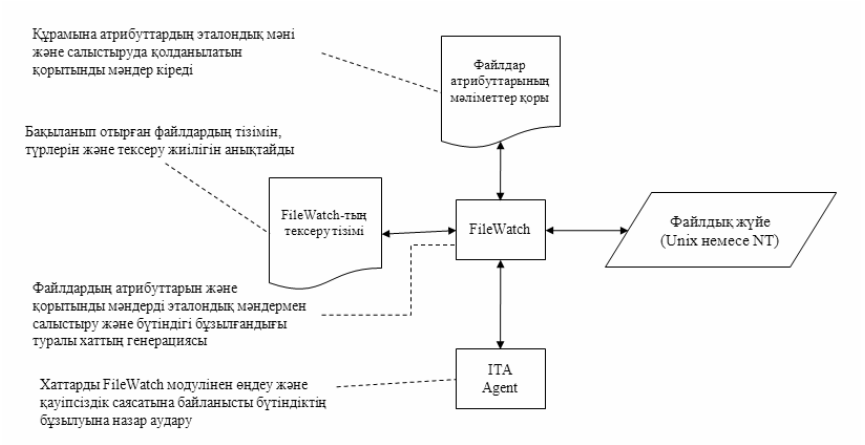
7.2-сурет. UNIX ОЖ-дегі ITA үшін оқиғалар жайындағы ақпараттардың көздері

Оқиғалар тіркейтін журналдағы мәліметтерді ««демон»» collogd жинайды және оларды программалық канал арқылы ITA агентіне жібереді. C2 қауіпсіздік аудитінің ішкі жүйесінен мәліметтер жинау - C2atd «демонының» қызметі болып табылады, ол бұл мәліметтерді ITA-дің ішкі форматына түрлендіреді және агентке жібереді. Ақпараттар көздерін сканерлеу бір секунд интервалында жүргізіледі.

Көптеген шабуылдарды жүргізудің сценарийі маңызды жүйелік файлдарды «трояндық программалармен» алмастыруды болжайды, программалардың вирус жұқтыруы немесе жүйеге «қосымша кіру» құру мақсатымен жүйелі конфигурациялық файлдарды модификациялау. ITA құрамында бақыланатын жүйеде ақпараттық бөліктердің және программалардың тұтастығын бақылау үшін FileWatch деп аталатын арнайы модуль бар, ол катологтар мен файлдарды модификациялау, жою және қосумен байланысты тұтастықтың бұзылуын анықтау әдісі болып табылады. Тұтастықтың бұзылуы осы файлдар мен каталогтардың атрибуттарын эталондық мәнмен салыстыру жолымен анықталады. Файлдың құрамының өзгерісін бақылау қорытынды қосындылар бойынша жүргізіледі. Файлдардың қорытынды қосындысын әртүрлі алгоритммен есептеп шығаруға болады, сонымен қатар хэш-қызмет MD5 көмегімен де.

FileWatch модулін функционалдаудың принципі 7.3 суретте кескінделген. Пайдаланушымен құрылған FileWatch List бақыланатын файлдар

тізімін, қабылданатын тексерулердің түрін және олардың периодтылығын анықтайды. Файл атрибуттарының мәліметтер базасы (File Attribute Database) FileWatch модулі бойынша құрылады және файл атрибуттарының және бақыланатын қосындының эталондық мәнін құрайды, олар тұтастықты тексеру үшін қажет. FileWatch модулі арқылы орындалатын тексеру нәтижелері туралы хабарлама ITA агенті арқылы жіберіледі, ол берілген қауіпсіздік саясатына сәйкес оларды өңдейді. ITA агенті FileWatch хабарламасын қабылдап және өңдей алуы үшін, сонымен қатар оларға әсер ету үшін арнайы қауіпсіздік саясаты белсенді болуы қажет (UNIX үшін UNIX Critical Files және Windows NT үшін NT Critical Files).



7.3- сурет. FiSeWatch модулінің көмегімен жүйелік файлдардың тұтастығын қадағалау

Intruder Alert қауіпсіздік саясаты ережелерді жинаумен сипатталады. Ережелер бірінші реттілік баяндауышында құрылған логикалық айтылуларды көрсетеді. Баяндауыштардың құралы бойынша жағдайды бақылау жағдайы анықталады, ал логикалық айтулар баяндауыштың жалған немесе шыншылдығына байланысты әсер ету әдісін береді.

Қауіпсіздік саясатының ережелері – бұл үш логикалық айтылымдар импликациясы: SELECT баяндауышы, IGNOR баяндауышы және логикалық айтылым ACTION. SELECT баяндауышы қадағаланып отырған жағдайдың пайда болу шарттарын анықтайды, IGNOR баяндауышы – осы шарттардың шектеуі, ал ACTION логикалық айтылымы пайда болған жағдайға әсер етуі бойынша 14 әрекеттерінің ішіндегі біреуін орындалуын болжайды.

Алгебра тілінде қауіпсіздік саясатының ережесінің қисыны тепе-теңдікпен орнатылады:

ACTION = SELECT → IGNOR.

7.1-кестеде берілген логикалық функцияның шындық кестесі қалай болатыны көрсетілген.

7.1-кесте

ACTION логикалық функцияның шындық кестесі

SELECT	IGNOR	ACTION
True	False	True
True	True	False
False	False	False
False	True	False

ACTION айтылымының шындығы әрекеттерді орындау қажеттілігін білдіреді, ол осы айтылымдарда көрсетілген. ACTION айтылымы қарапайым немесе құрамдас болып келеді, екінші жағдайда ол ∧ (логикалық «И») операциясымен бөлінетін бірнеше айтылымдардан тұруы мүмкін:

ACTION = Әрекет1 ∧ Әрекет2 ∧ ... Әрекет N, N ={ 1,14}.

7.2-кестесінде ITA-мен қолданылатын рұқсат етілмеген ену әрекетіне әсер ету әдісі сипатталған.

7.2-кесте

ITA программасымен қолданылған, рұқсат етілмеген ену әрекетіне әсер ету әдістері

Әдістің аталуы	**Тағайындалуы**
Execute Command	Орындалатын файл, файл сценарийі немесе операциялық жүйе бұйрығын орындау
Record To ITA View	Оқиғалар туралы мәліметтері бар жазбаны қауіпсіздік ITA менеджерінің мәліметтер базасына енгізу
Disable User Account	Қолданушының тіркелу жазбасын құлыптау
Run Shared Actions	ITA агентінде іске қосылған қауіпсіздік саясатының басқа ережелермен анықталатын әрекеттерді орындау

Қауіпсіздік саясатының ережелері жүйе болып жатқан оқиғалардың күрделілік дәрежесін анықтау мақсатында ранжирленеді. Әрбір ережеге 0 мен 100-дің аралығындағы нөмір беріледі. Қауіпсіздік саясат ережелерімен қарастырылатын барлық оқиғалар өздерінің басымдылық тәуелділігінде 7.3-кестесіне сәйкес үш күрделі деңгейге бөлінеді (ITA диаграммасында әртүрлі түстермен көрсетіледі).

7.3-кестесі

ITA программасымен қадағаланатын оқиғалардың басымдылық деңгейлері

Басымдылық	Күрделілік деңгейі	Қауіпсіздік қаупі
0-33	Жасыл	Тез арада әсер етуді қажет етпейтін күрделі емес оқиғалар
34-66	Сары	Әсер етуді қажет ететін маңыздылығы орташа күрделі оқиғалар
67-100	Қызыл	Тез арада әсер етуді қажет ететін және қауіпсіздікке үлкен қауіп төндіретін, маңыздылығы жоғары күрделі оқиғалар

ITA өніммен бірге орнатылатын әрбір қолдалатын операциялық жүйелер үшін қауіпсіздік саясаты алдын ала анықталған базалық жинақтарды құрайды. Алдын ала анықталған қауіпсіздік саясатының бір бөлігі ITA жүктемесінен кейін іске қосылады. Қалғандары қосымша баптауды қажет етеді.

Мысалы, ITA Reports саясаты ITA View–дан (ITA View сонымен қатар, ITA агенттерін желі бойынша оларға бұйрық жіберу жолымен басқаруға мүмкіндік береді) report командасын алған кезде программалық агенттің жұмысы жайлы есеп беруді генерациялайды. UNX Failed telnet саясаты Solaris 2.5 жүйесіндегі жойылған тіркеулердің сәтсіз әрекеттерін telnet сервисін қолдану арқылы айқындау қызметін атқарады, ал UNX System Problems саясаты бойынша түйінді мәселелер анықталады, олар жүйелік тапсырмаларды орындау кезінде, бақылау жүргізу томын сәтсіз операциялау, сұранысқа жауапты күту уақытының өтуі, MAC немесе IP мекен-жайларының қателігі сияқты кездерде туындайды. Windows NT ОЖ үшін NT SYN Flood саясаты «қызмет көрсетуден бас тарту» SYN Flood шабуылдарын іздейді, ал NT Guest User Logon саясаты жүйеге «Қонақ» атымен қолданушының жергілікті немесе жойылатын кіруі жағдайды тіркейді.

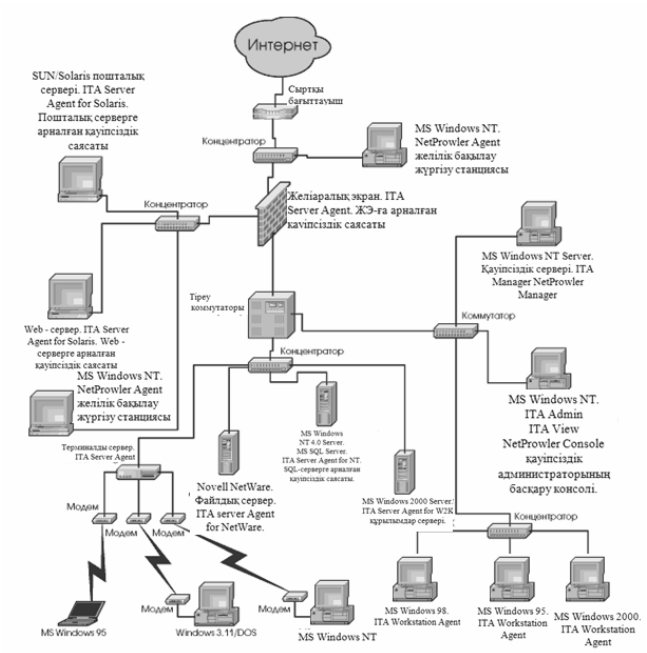
Алдын ала анықталған саясаттың бір бөлігін іске асыру алдында қосымша бапталған болуы қажет. Олардың арасында APACHE HTTP Start/Stop саясаты бар, ол Web-сервер Apache 1.1.1-дың жұмысты тоқтату және іске қосуды табатын және Cisco Config Change, Cisco v11. саясаты бағыттауыштың конфигурациясының өзгерісін анықтайтын.

7.5.3 Symantec IDS-ті қолдану мысалы

Internet-ке қосылған бірлескен желіні қорғауға қажетті Symantec компаниясының шабуылдарды анықтау құралының таралуының типтік схемасы 7.4-суретте келтірілген. IDS жеке компоненттерінің құрамы, конфи-

гурациясы және таралуы тәуекел талдауы және қауіпсіздікті зерттеу нәтижелері бойынша анықталады.

ITA агенттері бірлескен желінің барлық бақыланатын жүйелерінде орналасады, оған қоса, жұмыс станциялары және серверлер, жүйелік Журналдар мониторингін және қосымшалар журналын өткізеді, әртүрлі тосыннан іске қосылудың түрлерін табады. Станцияның қолданушы жұмысшылары, ереже ретінде, ақпараттық инфрақұрылымның критикалық элементі болып табылады. Сол себепті оларға агенттердің жеңілдетілген нұсқалары орнатылады, 7.4 суретте функциялау кезінде өтетін оқиғаларды қадағалау үшін келтірілген ITA Workstation Agents секілді.



7.4-сурет. Корпаративті желіні қорғау үшін Symantec компаниясының шабуылды айқындау құралының қолданылуы

Қолданбалы ішкі жүйелерді функционалау кезінде болатын оқиғаларды бақылап отыру үшін ITA желілік агенттерінде ЖЭ, пошталық пен Web-серверлік және де SQL-серверлері үшін арнайы қауіпсіздік саясаты іске қосылған.

Шабуылдарды анықтау жүйесінің ядросы ITA Manager функционалданатын қауіпсіздік сервері болып табылады. Қауіпсіздік серверінде желіде болып жатқан және агенттерден келіп түсетін оқиғалар туралы барлық

ақпараттар жиналады. Мұнда IDS-тің барлық конфигурациялық ақпараттары орналасқан, сонымен бірге шабуыл сигнатуралары және қауіпсіздік саясаттары. Қауіпсіздік серверінен оларға басқару хабарламаларын жіберу арқылы IDS-тің барлық агенттерімен басқару жүргізіледі.

Шабуылды айқындау жүйесін конфигурациялау, өзіндік шабуыл сигнатураларын және қауіпсіздік саясаттарын құру, аудиттің мәліметтерін қарау және талдау, сонымен қатар есеп беру генерациясы қауіпсіздік администраторының басқару консулінен жүргізіледі, оларда ITA Admin және ITA View-ді администрациялаудың графикалық тәсілдері орнатылады. Берілген қосымшалар администратордың қауіпсіздік серверімен өзара әрекетіне қажетті интерфейсті іске асырады.

7.6 Даму тенденциясы

Желілік шабуылдардан қорғану мәселесін шешу үшін қорғаныс объектілерін, мақсаттарын, тапсырмаларын және қорғаудың басты принциптерін анықтайтын, сонымен бірге ескерту және шабуылдарды анықтау және оларға әсер ету жұмыстарының құрамы мен жүйелілігін анықтайтын концепция қажет.

Сыртқы периметрге қорғанысты қамтамасыз етудің қарапайым және тиімді жолы SANS институтымен жарияланған он осалдылық (Top Ten List) тізіміне (http://www.sans.org/topten.htm) жүгіну болып табылады, олар шабуылға жиі ұшырайды (Берілген тізімде осалдылықтардың сипаттамасы және оларды жоюдың әдістері бар, олармен 80%-дан көп жағдайда желілік шабуыл жасайтын хакерлер қолданады.) Көптеген хакерлер нақты хосттардың тек соған тән осалдылықтарын іздеп қиналмайды. Оның орнына, шабуыл жасауға қажетті аз ғана тәсілдерді біле отырып, өздері білетін бір осал жерін табу үмітімен, олар жәй ғана желіні сканерлеп шығады. Қазіргі заманғы желілік сканерлер осы осалдылықтарды анықтай алады. Мұндай осалдылықтарды тауып және оларды жою қазіргі заманғы желіні бұзушылардың өмірін қиындатады. Енді олар бұзудың жаңа, өткірлеу түріне көшуге мәжбүр болды, жаңа әдістер мен тәсілдерді ойлап табу арқылы өздерінің шабуыл жасау тәсілдерін жаңартып, толықтырулары керек. Бұл бұзушылардың және олармен жасалатын шабуылдардың жалпы санын азайтады.

Қазіргі уақытта жиі шабуылданатын осалдылықтардың тізімі кеңейтілген және ол 20 шақты осалдылықты құрайды (http:/www.sans.org/top20.htm).

Әрине, ұсынылып отырған көзқарас толықтығымен ерекшеленбейді және желілік шабуылдардың көп түрлерінен қорағануды қамтамасыз ете алмайды. Желіні сыртқы шабуылдардан қорғаудың комплексті тұжырымдамасы келесі іс-шаралардың орындалуын болжайды:

- желілік енуді қадағалау саясатын жасап шығару;

- тәуекел мен осалдылықтарды талдау, қауіпсіздікті қамтамасыз ету жөніндегі қазіргі таңда бар шешімдерін және дұрыс тәжірибелерді қолдану;

- инфрақұрылым құру (жауаптыларды тағайындау, рөлдерді үлестіру және т.б.);

- қорғаныс жүйесін жобалау, орнатылған құрылғыларға және қорғаныс механизміне қойылатын талаптарды анықтау;

- қорларды бөлу, таңдап алынған қарсы әдістерді маңыздылық деңгейі және басым сипаттыларын іске асуы бойынша бөліп қарастыру (ранжировать);

- тексеру жүргізу және қабылданған қарсы әдістердің тиімділігін кейде сынақ жүргізу арқылы тексеріп отыру;

- шабуылды анықтау жүйесін және оларға жауап қайтаруды қалыптастыру және қолдау.

ҚОСЫМША. НЕГІЗГІ ТҮСІНІКТЕР ЖӘНЕ ТӘУЕКЕЛДЕРДІ БАСҚАРУДЫҢ АНЫҚТАМАЛАРЫ

Бұл қосымшада әртүрлі авторлармен және ұйымдармен қолданылатын тәуекелдері (риск) талдау тақырыбы бойынша, негізгі терминдердің анықтамалары [1, 8].

Тәуекелдерді базалық талдау (Baseline) – қорғаныстың базалық деңгейінің талаптарымен сәйкес жүргізілетін тәуекелді талдауы. Берілген деңгейге бағытталған тәуекелдерді талдаудың қолданбалы әдістері, әдетте ресурстардың бағалылығын қарастырмайды және бағалық өлшеулердің тиімділігін бағаламайды. Бұл кластың әдістері, ақпараттық жүйеге қауіпсіздіктің жоғары талаптары көрсетілмеген жағдайларда қолданылады

Тәуекелдерді толық (Full) **талдау** – АҚ саласындағы жоғарырақ талаптары бар ақпараттық жүйелер үшін тәуекелдерді талдау (қорғаныстың базалық деңгейіне қарағанда жоғарырақ). Бұл мынаған ұйғарым жасайды:

– ресурстардың бағалылығын анықтау;

– сезімталдық және қауіптің бағасын;

– тиісті контрмерді, олардың эффективтілігін таңдау.

Қауіп (Threat) – бүтіндіктің, ыңғайлылықтың, конфиденциялдықтың бұзылуларына себеп болатын, шарттар мен факторлардың жиынтығы.

АҚ қаупі (Threat) – қорғау объектісіне (ақпараттық ресурстар), қарсы бағытталып, қандай да бір әрекеттерді жасайтын (әрекет немесе әрекетсіздік), өзіне, иеленушіге немесе пайдаланушыға зиян тигізетін, қысу және/немесе ақпараттарды жоғалту кезінде пайда болатын, мүмкін болатын қауіп-қатер (потенциалдық немесе шынымен бар).

Қауіп көзі – потенциалды антропогенді, техногенді немесе апатты қауіпсіздік қаупін алып жүретіндер.

Қауіптердің әрекеті (threat action):

– қорғау жүйесіне шабуылдау.

Қауіптерді талдау (threat analysis):

– оқиғаның ықтималдығының бағалары және жүйедегі бұзу әрекеттерінің мүмкін болатын салдарын анықтау;

– жүйеге немесе оның қызмет нәтижелеріне жағымсыз әсер ететін барлық іс-әрекеттер мен оқиғалардың сараптамасы.

Салдар (шабуыл салдары) – өзінде бар факторлар (осалдықтар) арқылы жүйенің қауіп негізімен өзара әрекеті кезінде қауіптің мүмкін болу салдары.

Анықтамадан көрініп тұрғандай, шабуыл - бұл әрқашан қауіпті бар қылатын және зиян тигізетін «негіз-фактор» жұбы.

Осалдық (Vulnerability) – қауіптің пайда болуын мүмкін қылатын қорғау жүйесіндегі әлсіздік:

– әрекет ету объектісі бола алатын қорғаудағы әлсіздік (мысалы, қорғау жүйесінің реализациясында немесе жоспарлауда, талдауды дұрыс жүргізбеу салдарынан);

– ақпараттық жүйедегі әлсіздік немесе ақпаратпен байланысты, кері оқиғалардың реализациясына әкелуге қабілетті құраушысы (мысалы, қорғаудың жүйелік процедуралары, аппараттық реализация немесе басқарудың ішкі құралдары);

– қорғау процедураларындағы, ақпараттық жүйелерді жобалаудағы, жүйенің реализациясы кезінде, басқарудың ішкі жүйесінде және т.б. ақпараттық қауіпсіздік саясатын бұзуға қабілетті болу жағдайы бар әлсіздік;

–ақпараттық қауіпсіздік саясатының бұзылу себебі болып, ақпараттық жүйелерді жобалау кезеңіндегі кемшіліктер, оның реализациясы немесе оны басқару болып табылады;

– потенциалды шабуылдың объектісінде қорғаудың әлсіздігі (мысалы, талдау, жобалау, жүйені құруда немесе эксплуатация кезеңдерінде жұмыстың аяқталмауынан);

– әлсіздіктің бар болуынан, жобалаудың немесе жүйені құрудың қателіктерінен, АҚ жүйесін, желіні, қосымшаны немесе хаттаманы компроматтаушы, күтпеген, қаламаған оқиғаның болуы мүмкін;

– ақпараттық ресурстармен байланысты қауіптерді өндіруге болатын, жүйелік деңгейде бағдарламалық қамтамасыз ету компоненттерінде немесе ақпараттық жүйедегі әлсіздік;

– бағдарламалық қамтамасыз ету процедураларындағы, жүйелік жобада, басқару жүйесіндегі әлсіздік. Ол кездейсоқ немесе әдейі АҚ саясатын бұзылуына алып келуге қабілетті. Ақпараттық қауіпсіздікті қамтамасыз ету процедураларында, техникалық құралдар арқылы басқару жүйесінде немесе физикалық қорғаныстағы, қауіптердің реализациясына қабілетті қасиет немесе әлсіздік;

– қауіптерді іс жүзіне еңгізуге көмектесетін, ақпараттық жүйелер тобының немесе ресурстардың әлсіздігі;

– Ақпаратты өңдеудің жүйесін құрайтын, бағдарламалық қамтамасыз етудегі, мәліметтер ағынындағы, аппараттық құралдардағы әлсіздік. АҚ бағдарламалық-техникалық деңгейде қамтамасыз етудің автоматтандырылған жүйелеріндегі, администраторлық басқару жүйелерінде, құралдар орындарындағы, ақпаратқа санкияланбаған қол жетулердің қауіптерін реализациялауға немесе ақпаратты өңдеу процесінің критикалық маңызды бұзуларына әрекет ететін әлсіздік.

Осалдықты талдау (vulnerability analysis):

– Ұйымдардың тапсырмалары мен мақсаттарын қорғау әрекетінің нақтылығын анықтауға мүмкіндік беретін, систематикалық түрде жүргізілген ақпараттық жүйенің сараптамасы, қорғауды құрудағы қателіктерді идентифициялау, қорғау әрекеттерінің тиімділік бағасы үшін және олар-

дың реализациясынан кейін әрекеттілігін нақтылау үшін бастапқы мәліметтерді жинастыру;

– Ұйымдардың тапсырмалары мен мақсаттарын қорғау әрекетінің нақтылығын анықтауға мүмкіндік беретін, систематикалық түрде жүргізілген ақпараттық жүйенің сараптамасы, қорғауды құрудағы қателіктерді идентифициялау, қорғау әрекеттерінің тиімділік бағасы үшін бастапқы мәліметтерді жинастыру.

Тәуекел (risk):

– осалдықтың бар кезіндегі және белігілі бір жағдайлар немесе оқиғаларда қауіптің реализациясына алып келетін, қатердің пайда болуының нәтижелі мүмкіндіктері немесе күтілетін жоғалтулар;

– жүйенің белгілі бір осалдығының нақтылығынан белгілі бір қауіп пайда болуының мүмкіндігі;

– осалдықтың бар болуынан табылған қауіптің нәтижесіндегі шығындардың ықтималдығы;

– ақпараттық ресурстар үшін бір немесе бірнеше қауіптердің салдарынан шығындардың мүмкіндігі (қаржылық немесе іскерлік тәуекелдермен шатастырмау керек);

– осалдығы бар және потенциалды бұзушы оны қолданудың мүмкіндігі және қалауының бар болу жағдайы;

– ерекше осалдықтың қолданылу мүмкіндігі;

– ақпараттық ресурстардың осалдығының бар болуынан потенциалдың берілген қауіпте болуы. Осы потенциалдың пайда болуы кезінде ұйымдарға зиян тигізуі мүмкін;

– жүйенің ерекше осалдығының бар болуынан ерекше қауіптің орындалатын мүмкіндігі;

Тәуекелдерді талдау – қауіптерді, осалдықты, мүмкін болатын зияндарды, сонымен қатар қарсы шараларды анықтайтын процесс.

Тәуекелдерді бағалау (Risk Assessment) – тәуекелдердің теңестірулері, оларды сипаттайтын параметрлерді таңдау және осы параметрлермен бағаларды алу.

Тәуекел бағасы – тәуекелдің болуы мүмкін кезінде зияндардың өлшемі.

Тәуекелдердің ықтималдығы – қауіптердің және осалдықтардың кейбір комбинациясы пайда болуының нәтижесінде белгілі бір бағамен тәуекелдің оқиғасының туу ықтималдығы.

Тәуекелдердің көлемі (күтілетін зиян немесе тәуекелдер дәрежесі) – белгілі бір бағамен оқиғаның шығуы және осы оқиғаның болу ықтималдығының математикалық күтілуі (тәуекелдің бағасын тәуекелдің ықтималдығына көбейту).

Тәуекелдерді талдау (risk analysis):

– Тәуекелдердің теңестіру процесі, олардың шамаларын анықтау және қорғауды қажет ететін аймақтардың бөлінуі. Тәуекелдерді талдау – тәуекелдерді басқарудың бөлігі.

– Тәуекелдердің мөлшерін бағалаудың систематикалық процесі.

Тәуекелдердің теңестірілуі (Идентификация) – тәуекелдер және осалдықтар алдағы талдаулардың негізі ретінде, бизнес-мақсаттары қарастырылатын тәуекелдердің теңестірілуі процесі.

Тәуекелдерді басқару (risk management):

– жүйенің ресурстарына қарама-қарсы әсер етуге қабілетті басқару, теңестірілу процестері, оқиғаның ықтималдығының азаюы және шығарылуы;

– жүйенің ақпараттық ресурстарына тиетін, басқару, теңестірілу, оқиғаның ықтималдығының азаюы және шығарылуы теңестірілуді енгізетін процестер;

– қорғау құралдарының жарамдылық шарттары кезінде, ақпараттық жүйеге потенциалды әрекет етуге мүмкіндігі бар, қауіпсіздік қатерлерін азайту, басқару, теңестіру процесі;

– жүйенің жүйелік ресурстарына кері әрекет ету жағдайында болатын, басқару, теңестірілу процестері, оқиғаның ықтималдығының азаюы және шығарылуы. Бұл процесс тәуекелдерді талдаудан, «баға эффективтілік» параметрін талдау, таңдау, қауіпсіздік жүйе ішін сынау және құрылуы және қауіпсіздіктің барлық аспектілерінің зерттелуінен тұрады.

Тәуекелдерді жоспарлау есебі (risk treatment) – тәуекелдерді бағалауға негізделген, тәуекелдерді басқару жүйесін жоспарлау процесі.

ӘДЕБИЕТ

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность - М.: ДМК Пресс, 2005. – 384 с.
2. http://www.bsi-global.com - Британский институт стандартов.
3. http://www.bsi.bund.de/gshb/english/menue.htm - IT Baseline Protection Manual. Standard security safeguards.
4. http://www.bsi.bund.de/fehler/index.htm - сайт Германского института стандартов в области информационных технологий.
5. http://csrc.nist.gov – сайт ресурсного центра компьютерной безопасности института стандартов США (NIST).
6. X/Open Baseline Security Services Specification (XBSS). C529, X/Open company, 1996. http://www.opengroup.org/public/tech/security/bsec96/download.htm.
7. Information Technology Security (ITS). Minimum Baseline Protective Resuirements. http: //esdis.dsfanasagov/security/req/basereq/basereqlist.htm.
8. http://www.garlic.com/~lynn/secure.htm - глоссарий по информационной безопасности.

МАЗМҰНЫ

Оқу басылымы

Уалшер Ануарбекұлы Төкеев
Берік Бақытжанұлы Ахметов

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БАСҚАРУ

Оқу құралы

Редакторы *Керімше Сәбит*
Мұқабасын көркемдеген *Ринат Скаков*

ИБ № 5378

Басуға 02.08.2011 жылы қол қойылды. Пішімі 60х84 1/16. Көлемі 10,06 б.т.
Офсетті қағаз. Сандық басылыс. Тапсырыс № 662. Таралымы 100 дана. Бағасы келісімді.
Әл-Фараби атындағы Қазақ ұлттық университетінің «Қазақ университеті» баспасы.
050040, Алматы қаласы, әл-Фараби даңғылы, 71.
«Қазақ университеті» баспаханасында басылды