

## **8-ші дәріс. Қауіпсіздік жүйелерінің дұрыстығын зерттеу; қорғау механизмдерін жобалау және құрастыру әдістері; тұтастықты бақылау саясатының моделі.**

**Ақпараттық қауіпсіздік жүйесін жобалау** ақпаратты қорғау жүйесі мен автоматтандырылған жүйенің архитектурасы бойынша техникалық талаптардың әзірленген қауіпсіздік саясаты негізінде, сондай-ақ ақпараттық қауіпсіздік жүйесінің жобалық құжаттамасын әзірлеуден тұрады.

Ақпараттық қауіпсіздік жүйесін жобалаудың басты мақсаты - қолданылатын технологиялар тұрғысынан да, бағаның алынған қауіпсіздік дәрежесіне ең жақсы арақатынасы бойынша да оңтайлы интеграцияланған жүйені дамыту. Ақпаратты қорғаудың интеграцияланған жүйесінің жоғары тиімділігіне оның барлық компоненттері жоғары сапалы шешімдермен ұсынылған, біртұтас кешен ретінде жұмыс істеген және орталықтандырылған басқару (**слайд**) ие болған кезде қол жеткізуге болады.

Ақпараттық қауіпсіздік жүйесінің **құрылымына** келесі ішкі жүйелер кіреді (**слайд**):

- рұқсатсыз кіруден қорғау;
- есептік жазбалар мен кіру құқықтарын басқару;
- кешенді антивирустық қорғау;
- желіаралық экрандау;
- басып кіруді анықтау, қауіпсіздікті бақылау және талдау;
- криптографиялық қорғау;
- ақпараттық қауіпсіздік құралдарын басқару;
- коммутацияланған инфрақұрылым мен сымсыз желілердің қауіпсіздігін қамтамасыз ету;
- ақпараттық ресурстарды пайдалануды бақылау;
- ақпараттық қауіпсіздік оқиғалары мен инциденттерін басқару;
- ақпаратты қорғау тиімділігін бақылау;
- қорғау құралдарының үздіксіз жұмыс істеуін қамтамасыз ету.

Барлық қажетті пайдалану және ұйымдастыру құжаттамасын жасай отырып, ақпараттық қауіпсіздікті қамтамасыз етудің кез-келген күрделі жүйелерін жобалау тәжірибесі бар.

**Жобалау келесі қадамдардан тұрады (слайд):**

- ақпараттық қауіпсіздік жүйесінің (АҚЖ) архитектурасына арналған шешімдерді әзірлеу;
- АҚ және бақылау құралдарын әзірлеу;
- АҚЖ техникалық жобасын (дизайнын) әзірлеу ;
- АҚЖ жұмыс құжаттамасын әзірлеу;
- АҚЖ арналған техникалық және бағдарламалық құралдарды жеткізуге техникалық құжаттаманы дайындау және ресімдеу;
- ақпаратты қорғау жөніндегі нормативтік құжаттардың талаптарын ескере отырып, АҚ үй-жайларын жобалау;
- автоматтандырылған жүйеде АҚЖ қолдау тәртібін әзірлеу;
- АҚЖ енгізу тәртібі мен кезеңдерін әзірлеу, тұтынушыға ақпараттық қауіпсіздік жүйелерін енгізу кезінде кеңес беру.

Кез-келген нақты мақсаттарға жету үшін қажет болатын жеке ішкі жүйелерді іске асырудың мүмкіндіктері бар. Ақпараттық қауіпсіздіктің бөлек ішкі жүйелері: CiscoSystems, Oracle, CheckPointSoftwareTechnologiesLtd, Microsoft, CryptoPro, S-Terra, NIP Informzashita, Kaspersky Lab, WatchGuard, GFI және т.б. негізінде жүзеге асырылады.

Ақпараттық қауіпсіздік құралдарын қолданудан басқа, операциялық жүйелерде, мәліметтер базасында және желілік жабдықта ақпараттық қауіпсіздіктің орнатылған тетіктерін пайдалануға болады.

Жобалау **нәтижесі** таңдалған техникалық шешімдердің сипаттамасын, ақпаратты қорғау құралдарын, оларды таңдаудың негіздемесін, сондай-ақ қажетті жабдық пен Программалық қамтамасыз ету ерекшеліктерін қамтитын **АҚЖ-ның жұмыс техникалық жобасы** болып табылады.

Қорғалған АЖ (автоматтандырылған жүйелер) құру әдістерін қарастырайық. Бұл әдістерді шартты түрде екі топқа бөлуге болады (**слайд**):

- **АЖ бойынша ерікті байланысқа жататындар:**

- иерархиялық әдіс;
- дұрыстығын зерттеу және тексеру (верификация).

- **тек қорғаныс жүйелеріне арналған (қауіпсіз жүйелер теориясы).**

Абстракция принципіне сәйкес, АЖ жобалау кезінде әзірлеушілер кем дегенде екі жолмен жүре алады: аппаратурадан «жоғарыға» - АЖ ұсынатын виртуалды машинаға немесе виртуалды машинадан «төменге» - нақты жабдыққа. Бұл жобалаудың екі негізгі әдісі - төменнен жоғары және жоғарыдан төмен әдіс. Қалған әдістер осы екі әдіс негізіне жасалады немесе олардың тіркесімі болып табылады.

«**Төменнен жоғары**» әдісі жүйенің негізгі аппараттық құралынан жобалауды көздейді. Жобалау кезінде модульдер бірқатар қабаттарға бөлінеді, ал виртуалды жүйенің нөлдік қабаты аппараттық құрал арқылы қалыптасады. Қажетті бір немесе бірнеше қасиеттерді іске асыратын қабаттар қажетті виртуалды машина алынғанға дейін дәйекті түрде қосылады.

«**Төменнен жоғары**» әдісінің **кемшіліктеріне** мыналар жатады:

- аппаратура, микропрограммалар немесе программалар көмегімен АЖ компоненттерін іске асыру тәсілін таңдау туралы шешімді басынан бастап қабылдау қажеттілігі, оны жасау өте қиын;
- аппаратураны әзірлегеннен кейін ғана АЖ жобалау мүмкіндігі;
- нақты АЖ мен ТТ-да анықталған(техникалық тапсырма) арасындағы алшақтық.

«**Жоғарыдан төмен**» әдісін (иерархиялық әдіс) қолданған кезде олар қажетті қасиеттері бар АЖ-ны білдіретін виртуалды машинадан шығады және виртуалды жүйенің қабаттарын жабдыққа дейін дәйекті түрде дамытады. Бұл жағдайда жобалау келесі ретпен жүреді.

Жоғарғы қабаттың АЖ компоненттерінің сипаттамасының абстракция деңгейі анықталады. Әрі қарай, кейбір қарабайыр ұғымдарды қолдана отырып, оларды жүзеге асыру үшін компоненттер жеткілікті түрде анықталған-анықталмағанына талдау жүйелі түрде жасалады. Егер жоқ болса, онда әр компоненттің әр функциясы абстракцияның төменгі деңгейіне сәйкес келетін келесі қабаттың құрамдас

бөліктерінің функцияларымен ұсынылады және оларды жүзеге асыру мүмкіндігіне талдау қайтадан жасалады. **Иерархиялық әдіспен құрылымдық принциптерді, модульдік дизайн принципін қолданған жөн.**

**Құрылымдық принцип** негізгі болып табылады және көптеген іске асырудың негізін құрайды. Осы принципке сәйкес жобалау үшін тек үш негізгі құрылым (**слайд**) қажет:

- функционалды блок;
- жалпыланған циклды құру;
- екі түрлі шешім қабылдауды құру.

**Ресми модельді қолданудың басты артықшылығы – оның көмегімен модельденген жүйенің ерекшеліктерін зерттеу мүмкіндігі.** Формальды даму әдісін математикалық модельге сүйене отырып, содан кейін модельді зерттей отырып, жүйенің іс-әрекетінің кейінгі кезеңдерге дейін көрінбейтін қыр-сырын анықтауға болады.

Жобалаудың мақсатты нысаны АЖ болғандықтан, модель АЖ-ның өзін немесе оның іс-әрекетін, яғни АЖ жұмысының сыртқы көріністерін сипаттай алады. АЖ моделімен салыстырғанда АЖ іс-әрекетін сипаттайтын модельдің бір маңызды артықшылығы бар – оны орындаушылар да, тапсырыс берушілер де тексеріп, бағалай алады, өйткені тұтынушылар АЖ қалай жұмыс істейтінін білмейді, бірақ олар не істеу керектігін ұсынады.

**Осындай модельдеу нәтижесінде тапсырманың бастапқы орнатылуына қатысты сипаттамалардың дұрыстығын тексеруге болады, яғни Техникалық тапсырма.**

Бұдан басқа, ерекшелік оны пайдаланудың барлық ықтимал (немесе жоспарланған) жағдайлары кезінде объектінің «сыртқы» іс-әрекетінің толық сипаттамасы болған жағдайда, дұрыстық критерийлері жеткілікті деп есептеледі.

Жоғарыда айтылғандай, АЖ-ны, әсіресе оның ақпараттық қауіпсіздік жүйесін білдіретін компоненттерін әзірлеу кезінде ақаулардың болмауына нақты кепілдік беру және жүйенің формальды тәсілдері және жүйенің талаптарға сәйкес жұмыс істейтіндігі туралы дәлелдеу қолданылады.