Лекция 15. Қорытынды Компьютерлік жүйелердің қауіпсіздігі

Жергілікті желілерді қорғау.

Жеке ақпаратты қорғау бағдарламалық құралдары

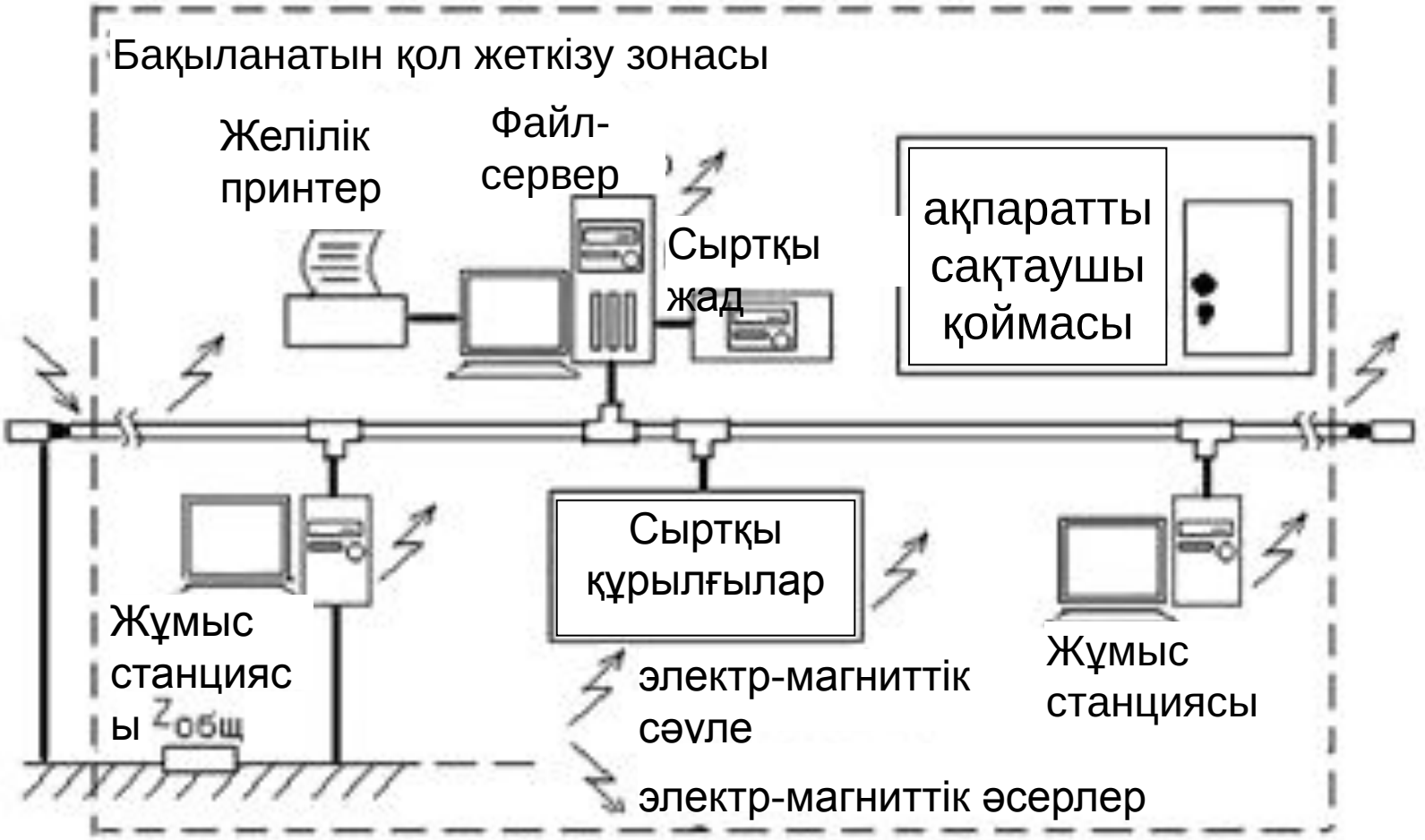
Жергілікті желілерді қорғау

- Ғимарат ішіндегі мекеменің бөлімдері арасында сенімді ақпарат алмасуды ұйымдастыру және деректер қорын ортақтасып пайдалануға мүмкіндік беретін компьютерлік желіні жергілікті дейді
- локальды желісі зерделеніп оның функциялары анықталады
- ақпараттың қауіпсіздігін қамтамасыз ету құралдары зерттеледі, таңдалады және әдістері өңделеді
- _Ақпараттық қауіпсіздік саясатын жоспарлап берілген сенімділікті қамтамасыз ететін шараларын белгілеу және тиісті құралдармен қамтамсыз ету

Желідегі ақпаратты қорғау

- Дербес компьютердегі жұмыстан желідегі жұмысқа көшу келесі себептермен ақпаратты қорғау күрделендіреді:
- 1) желіде пайдаланушылардың үлкен саны және олардың өзгергіш құрамы болады. Пайдаланушының аты және паролі деңгейінде қорғау бөтен адамдардың желіге кіруден қорғамайды;
- 2) желінің маңызды ұзындығы және желіге ену көптеген потенциалды каналдарының бар болауы;
- 3) аппараттық және бағдарламалық қамтамасыз етудегі белгіленген жетіспеушіліктері пайдалану барысында анықталады.

Проблема өткірлігін, ұзындығы үлкен желінің бір сегменті көрсетеді



Қасақана әрекеттерді қақпайлау құралдары

- Бүтіндей ақпаратты қорғауды қамтамасыз ету құралдарын орындау тәсілі бойынша қасақана әрекеттерді қақпайлау мына топтарға бөлуге болады:
- 1) техникалық (аппараттық) құралдар.
  - Техникалық құралдардың артықшылығы олардың сенімділігі, субъективті факторлардан туәелсіз, модификацияға биік тұрақтылығы.
  - Әлсіз жақтары – иілгіштігі төмен, салыстырмалы көлемі және салмағы үлкен, құны жоғары.
- 2) бағдарламалық құралдар
  - пайдаланушыларды сәйкестендіру, қол жеткізуді бақылау, ақпаратты шифрлеу, қалған (жұмысшы) уақытша файлдан ақпараты өшіру, қорғау жүйелерін тестлік бақылау бағдарламаларынан құралады.

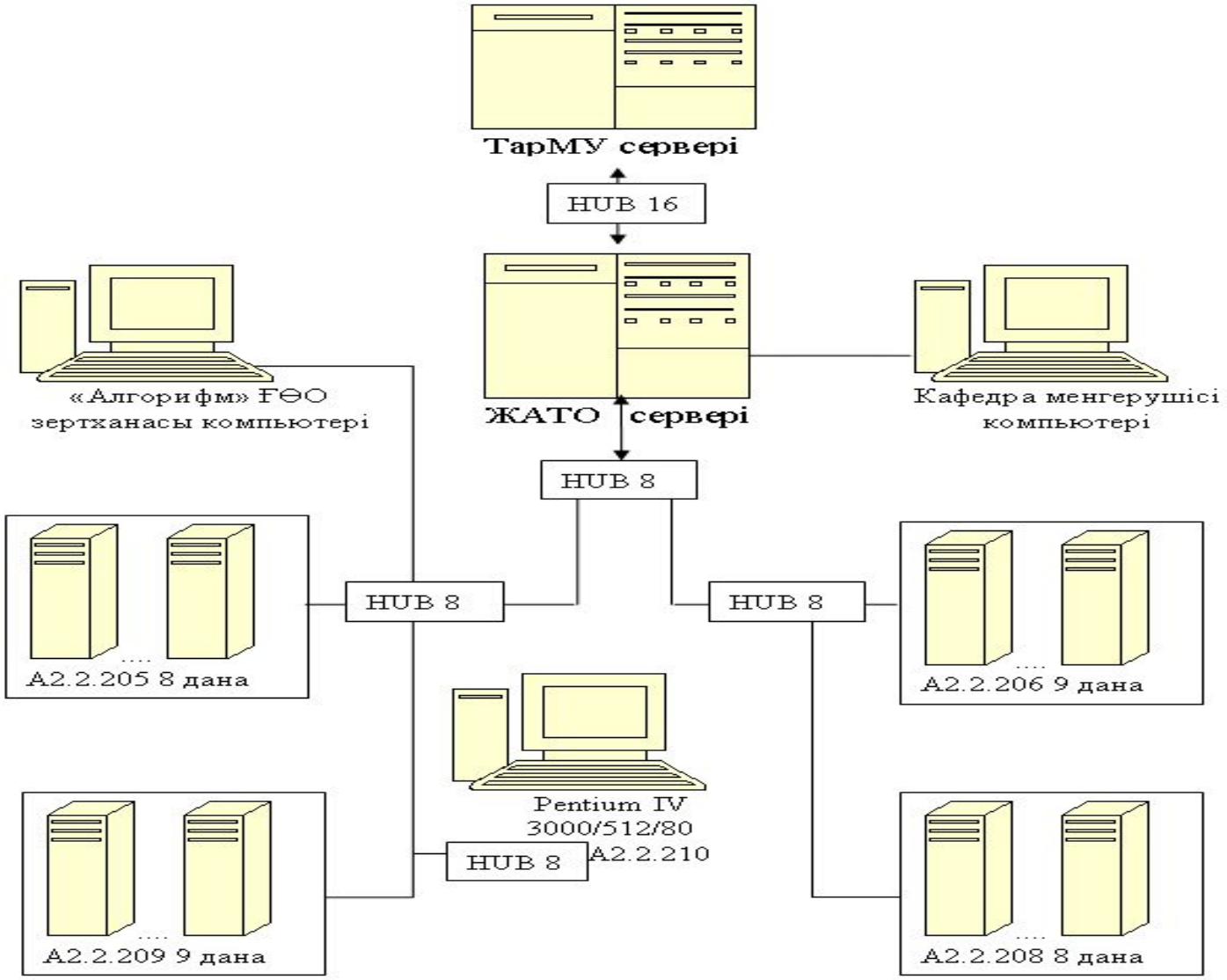
Бағдарламалық құралдар

- Бағдарламалық құралдардың артықшылығы:
  - әмбебаптық, иілгіштік, сенімділік,
  - құруы қарапайым,
  - модификацияға және дамуға қабілеттіліктері.
- Жетіспеушіліктері
  - желінің функционалдылық шектелуі,
  - файл-сервер және жұмысшы станциялардың ресурстарының бір бөлімін қолдану,
  - кездейсоқ немесе қасақана өзгертуге биік сезгіштік, компьютерлердің үлгісіне тәуелділігі
- 3) араласқан аппараттық-бағдарламалық құралдар қасиеттері аралық

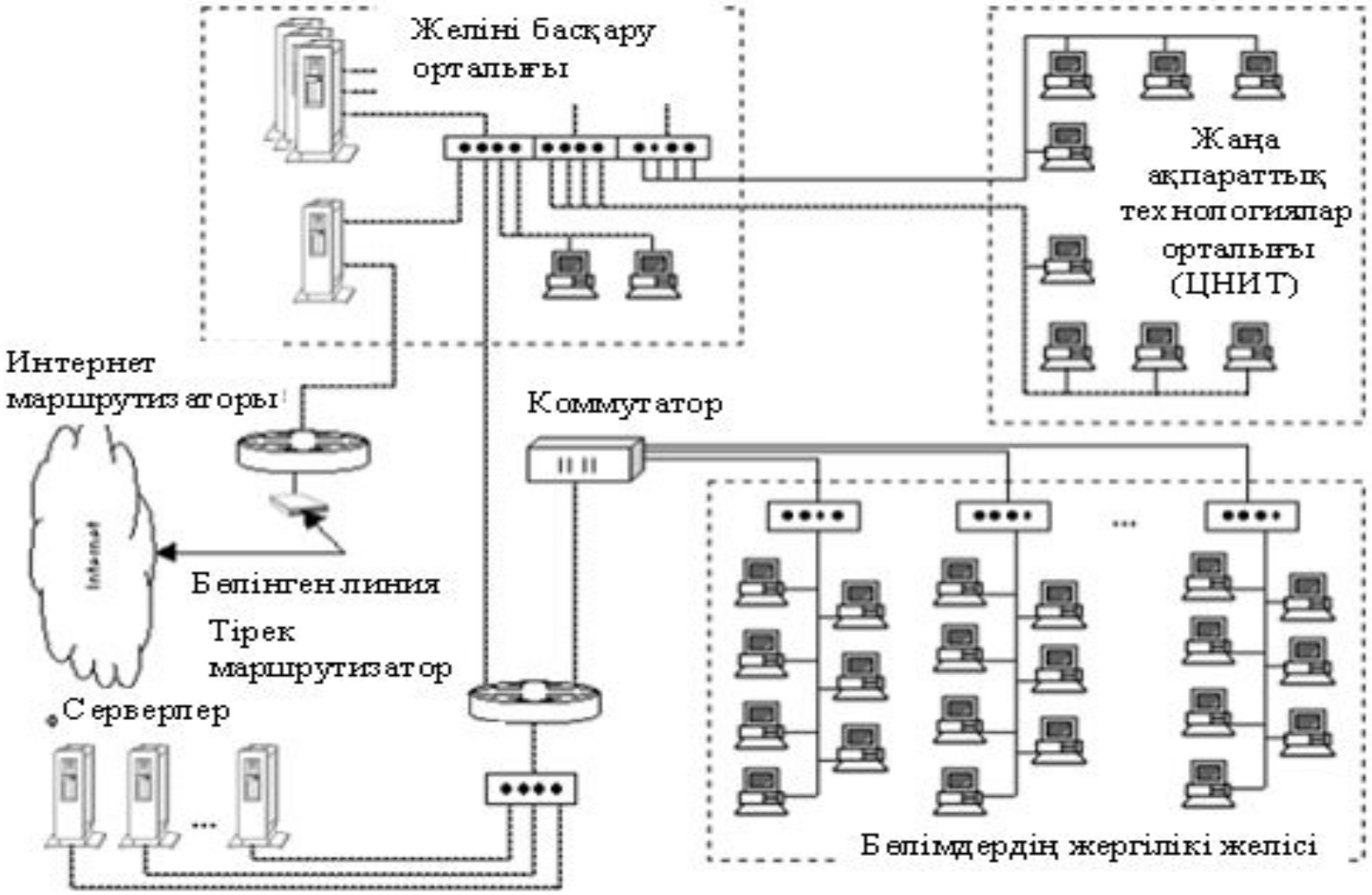
Ұйымдық құралдар

- 4) ұйымдық құралдар:
  - ұйымдық - техникалық (компьютерлер орналастыру, кабелдік жүйе салу)
  - және ұйымдық-құқықтық құралдардан тұрады.
- Оладың артықшылықтары:
  - әр текті проблемалардың жиынын шешуге мүмкіндік етеді,
  - орындауы қарапайым,
  - желідегі жағымсыз әрекеттерге жылдам сезінеді, модификация және даму мүмкіншіліктері шектелмеген.
- Жетіспеушіліктері
  - жалпы ұйымдардағы субъективті факторларға биік тәуелділігі.

«Компьютерлік жүйелер» кафедрасы жергілікті есептеу желісінің сұлбасы

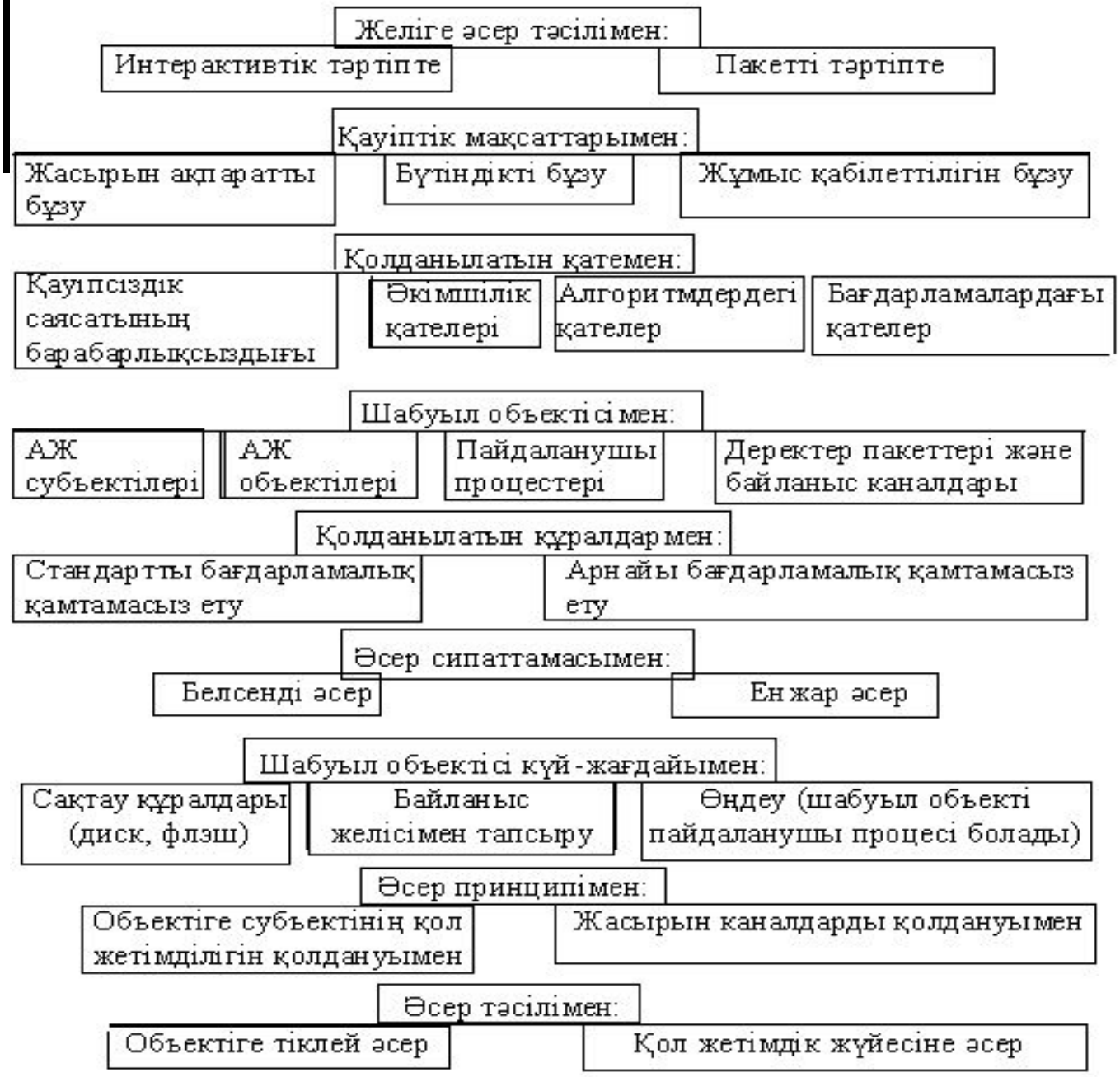


ТарМУ компьютерлік желісі



OSI эталондық моделінің жеті деңгейлері

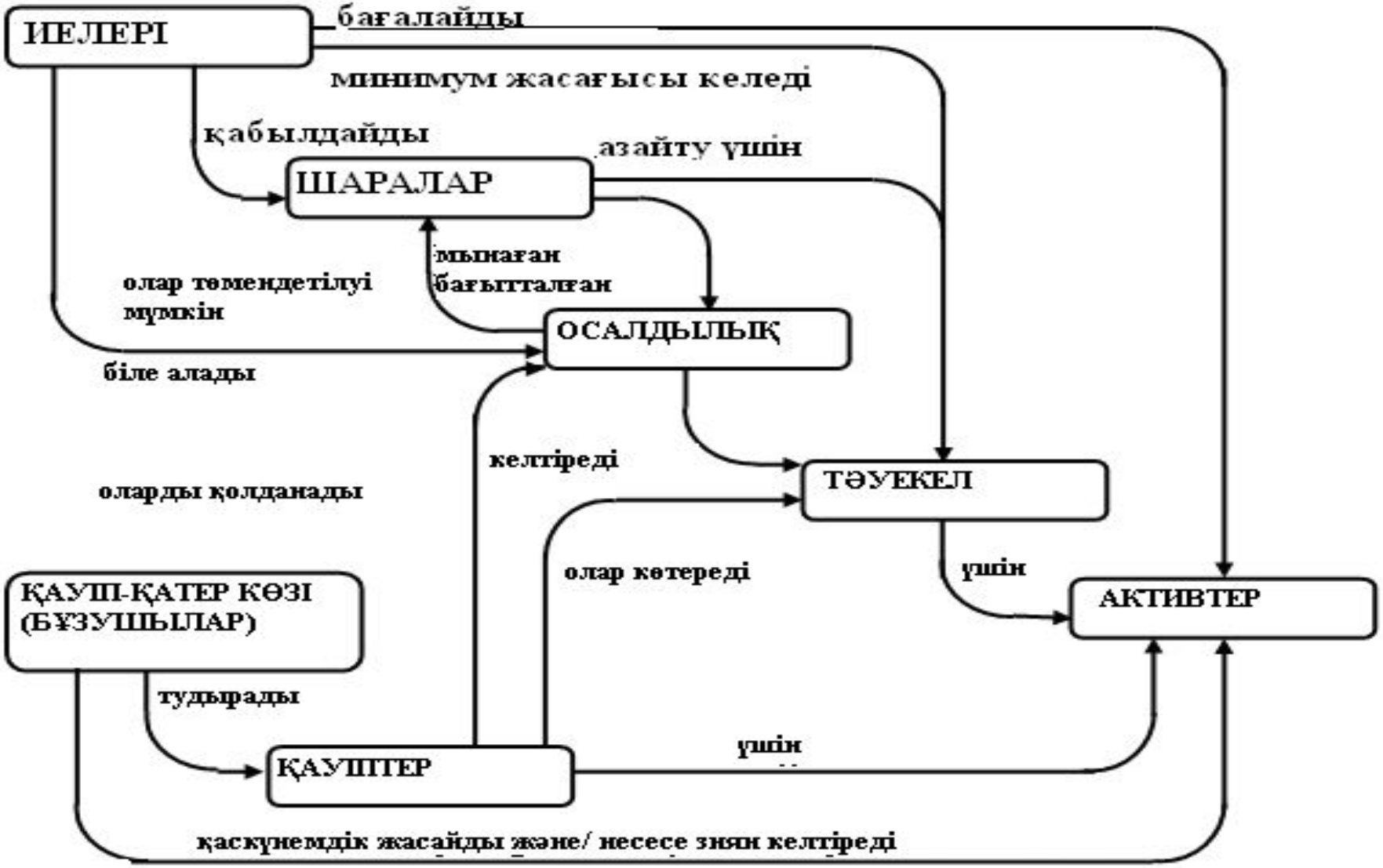
Қауіпсіздік қатерлерінің жіктелуі



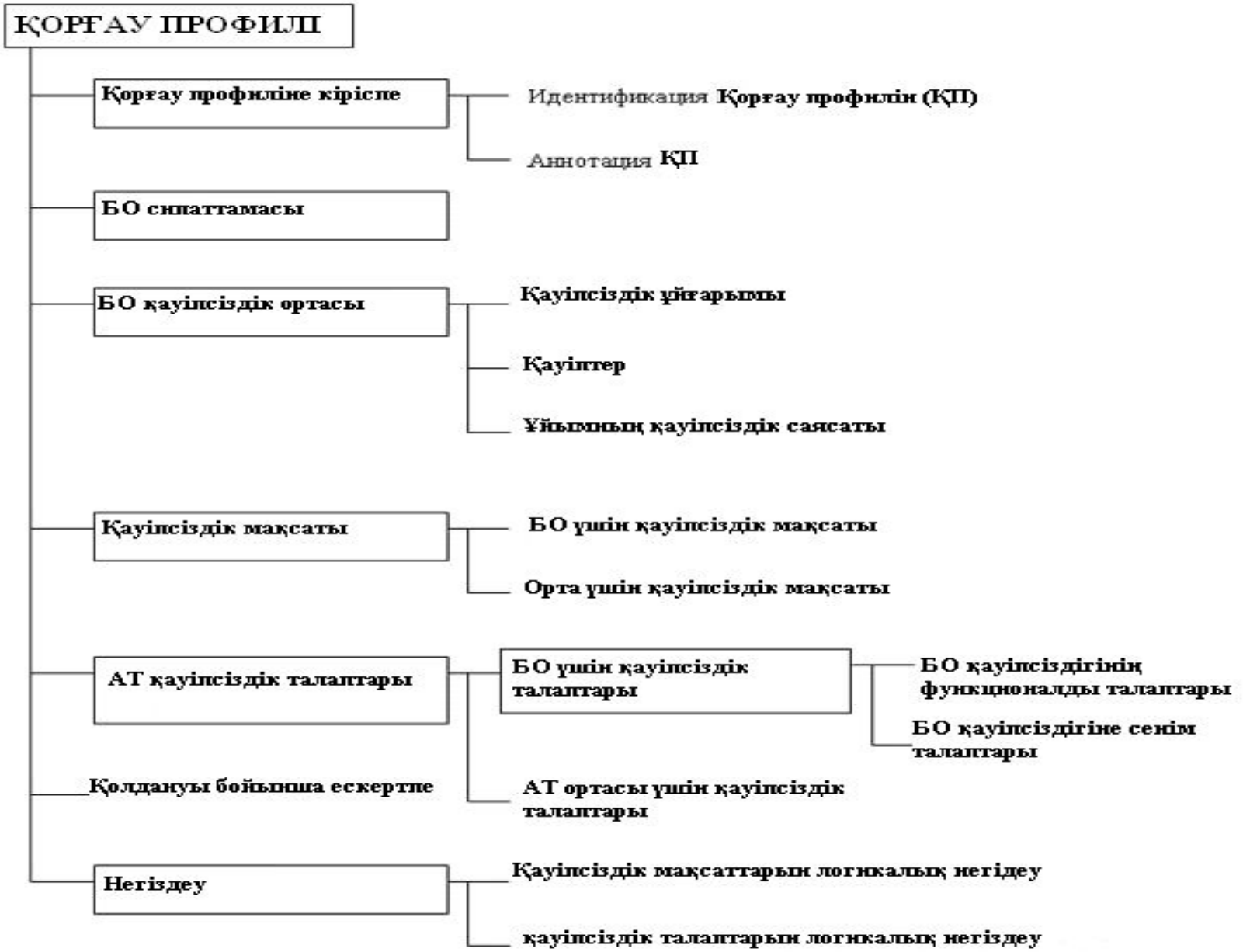
Internet ақпараттық қауіпсіздік қауіптері

Қауіптер	Орындалу ықтималдығы
Ұқыпсыздық	0,188
Қарақшылық	0,166
Нақты емес немесе ескірген ақпарат	0,159
Деректердің кемуі «ағып кетуі»	0,159
Әріптестердің бір-біріне "әзілі"	0,150
Сәулелендуді бақылау	0,133
Деректерге және бағдарламаларға әдейі зақым келтіру	0,129
Аутентификацияны бұзу	0,129
Шамадан артық жүктеу	0,119
Дұрыс емес маршрутизация	0,106
Аппараттық тоқтап қалу	0,090
Бұрмалау	0,080
Желілік талдауыштар	0,074
Алаяқтық	0,058
Өрттер және басқа апаттар	0,043
Арамдық	0,033
"Логикалық бомбалар"	0,032
Ұрлық	0,032
Ақпаратты тоқтатып қою	0,016
"Жасырын жолдар және өтетін тесіктер"	0,010

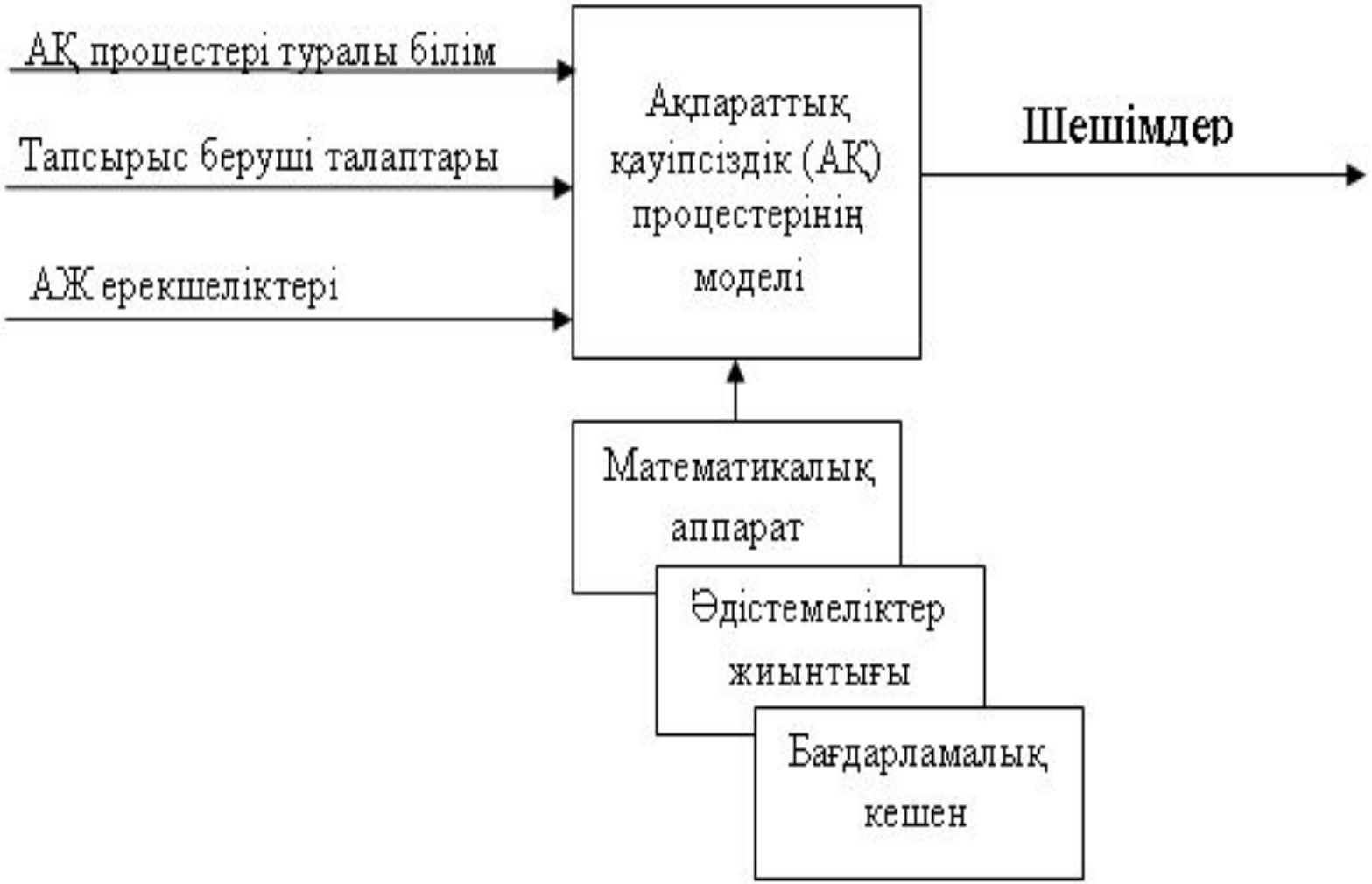
Желінің ақпараттық қауіпсіздігін бағалау критерийлері



Қорғау профилінің құрылымы

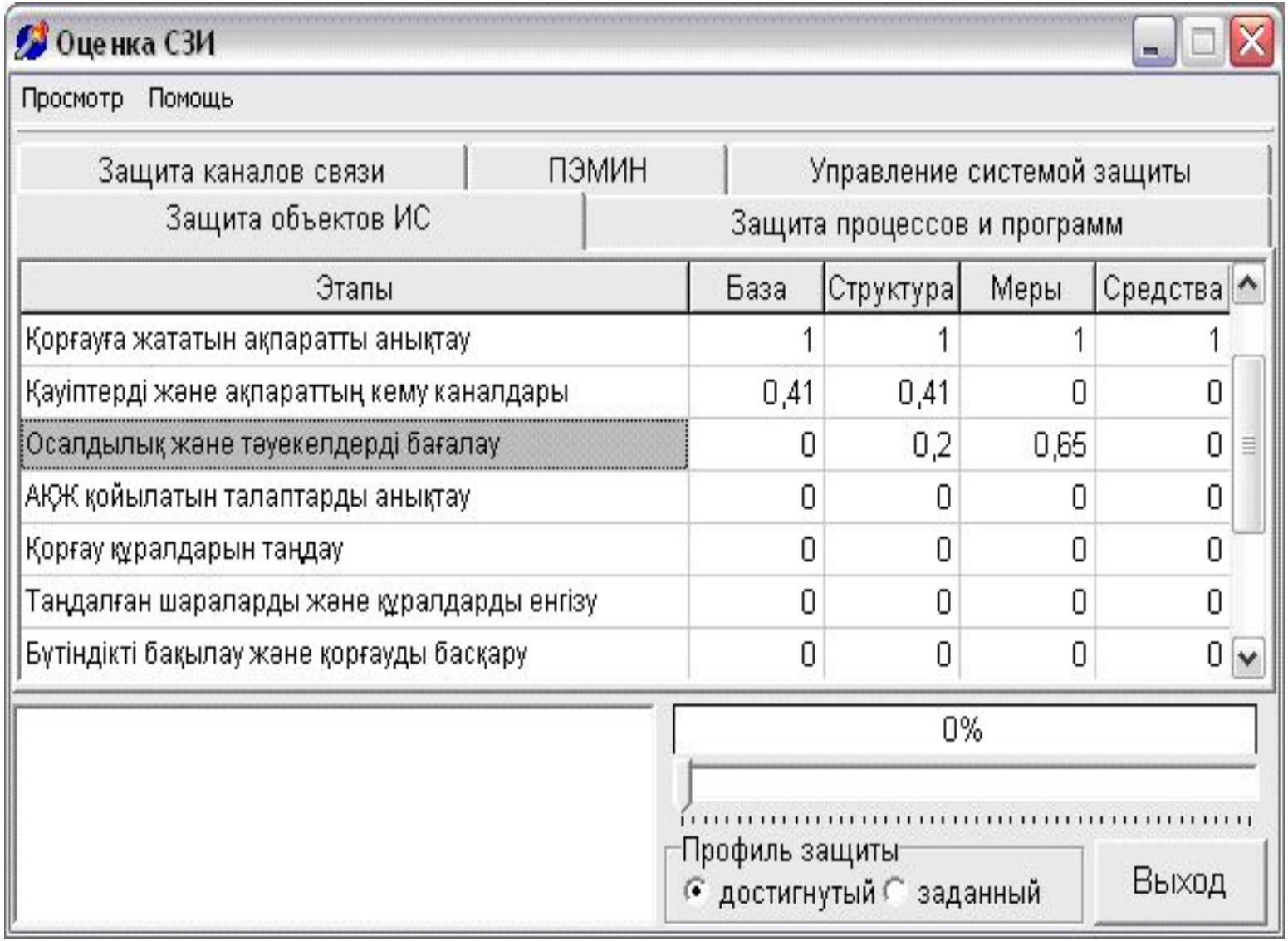


Ақпараттық қауіпсіздік жүйесінің моделі



АҚЖ моделіне қойылатын талаптар

АҚЖ тиімділін бағалау бағдарламасы интерфейсі



ҚОРЫТЫНДЫ

- Өңделетін ақпараттың көлемінің өсуі және пайдаланушылар шеңберінің кеңейуі ақпараттық жүйенің ресурстарына және деректеріне бекітілмеген қол жетімдік жаңа мүмкіншіліктерге және олардың жоғары осалдылығына әкеледі.
- Біріншіден, қорғау механизмдарын ақпараттық жүйе өңдеуімен бір уақытта жобалау қажет, бұл олардың келіспеушіліктерінен құтқарады, есептеуіш ортаға дер кезінде интеграциялау мүмкіншілігін береді және шығындарды қысқартады
- Екіншіден, бірыңғай ақпаратты қорғау жүйесі рамкаларында кешенді қорғау сұрақтарын анық қарауға болады
- Қауіпсіздік екі профилі қарастырылады: қойылатын талаптар және нақты қол жеткен. Қауіпсіздікке қойылатын талаптардың профилін АҚЖ құруға тапсырыс беруші алдын ала анықтайды
- АҚЖ тиімділігі (сапасы) оған қойылған талаптардың орындалу дәрежесімен (толықтығымен) анықталады.

АҚ шығындарын есептеу

- Зерттеулерге қарағанда компанияның батыс мемлекеттері АҚ-ке АТ- бюджетінің 5% шығындайды, ал Ресейде арнайы қызметтің бағалауы бойынша «Инфофорумда *[2008 г.]*» тек 0,5%-н шығындайтынын хабарлады.
- “Егер біз компанияның қаржы директорына АҚ-ке не үшін ақша бөлетінімізді айтып, түсіндіре алсақ, біз де АҚ-ке 5% шығын бөле алатын едік”.

Владимир Мамыкин, Microsoft фирмасының Ресейде және ТМД елдеріндегі ақпараттық қауіпсіздік бойынша директоры

АҚ ғылыми зерттеу облысындағы негізгі бағыттар мен басымды мәселелер

- «Жүйенің қауіп-қатер қауіпсіздік моделін құру және оларды жүзеге асыру әдістерін, әлсіз критерийлерін анықтау және жүйенің тұрақтылығына деструктивті әсер ету, методология және методикалық шығындарды бағалау аппаратын құру.
- Экспертиза жүргізу үшін әдістер мен құралдарды құру және ақпаратты қорғау сапасын бағалау, ақпараттық ресурстарды, сонымен қатар негізгі жалпы жүйелік программалық құралдарды ақпараттық қауіпсіздікке сай екендігін тексеру.

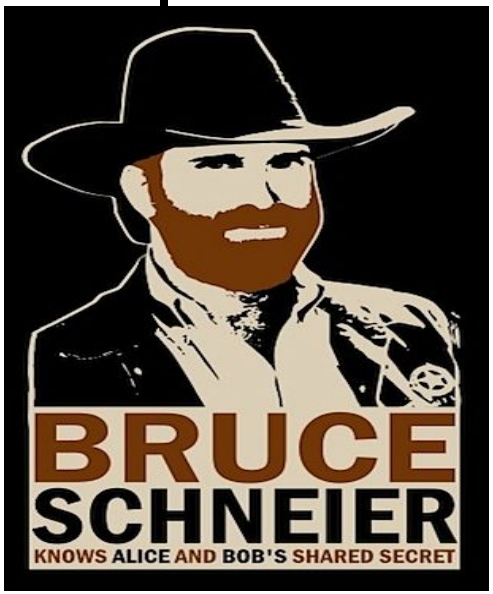
Бағалау әдістері

- Криптотұрақтылықтың сараптамасы;
- В.П. Иванов құрастырған санкционирленбеген енуден ақпараттың математикалық қорғалуының бағасы;
- Ойындардың теориясы;
- Ақпараттық тәуекелділіктердің сараптауының және бақылауының әдістері мен құралдары;
- Криптохаттамалардың формальды сараптамасының әдістері

Бағалау әдістері

- Криптотұрақтылықтың сараптамасы;
- В.П. Иванов құрастырған санкционирленбеген енуден ақпараттың математикалық қорғалуының бағасы;
- Ойындардың теориясы;
- Ақпараттық тәуекелділіктердің сараптауының және бақылауының әдістері мен құралдары;
- Криптохаттамалардың формальды сараптамасының әдістері

Криптотұрақтылықтың сараптамасы



- «… it becomes increasingly clear that the term "security" doesn't have meaning unless also you know things like *"Secure from whom?"* or *"Secure for how long?“*»

Бағалау әдістері

Криптотұрақтылықтың сараптамасы;

- Ойындардың теориясы;
- В.П. Иванов құрастырған санкционирленбеген енуден ақпараттың математикалық қорғалуының бағасы;
- Ақпараттық тәуекелділіктердің сараптауының және бақылауының әдістері мен құралдары;
- Британиялық CRAMM (Insight Consulting, Siemens)
  - Американдық RiskWatch (компания RiskWatch)
  - Ресейлік ГРИФ (компания Digital Security).
- Криптохаттамалардың формальды сараптамасының әдістері

Ойындар теориясы (Bennet S. Yee)

Ақпараттық тәуекелділіктердің сараптамасы: CRAMM

- **1: қорғалатын ресурстардың идентификациясы және бағалылығын анықтау**
- **2:** АҚ сферасындағы қауіп-қатердің **идентификациясы және бағалылығы, қорғалатын жүйенің әлсіздігін бағалау және іздеу**
- **3:** көрсетілген тәуекелдіктерге қарсыь нұсқалардың өлшеу генерациясы:
  - жалпы мінездемелі пікір;
  - нақты пікір;
  - Осы жағдайдағы қорғанысты ұйымдастыру мысалы.
- **Әдістің кемшіліктері**:
  - СКЗИ спецификасын есептемейді !

Криптохаттамалардың формальды сараптамасының әдістері

- **Әдістердің класы**:
  - Дедуктивті әдістер
  - Күй сараптамасының әдістері
  - Статистикалық сараптаманың әдістері

- **Кемшіліктері**:
  - Сөйлемдегі реализациядан детальдардан абстрагирленеді, сонымен қатар қолданылған шифрлеу әдісі идеальды болып табылады.

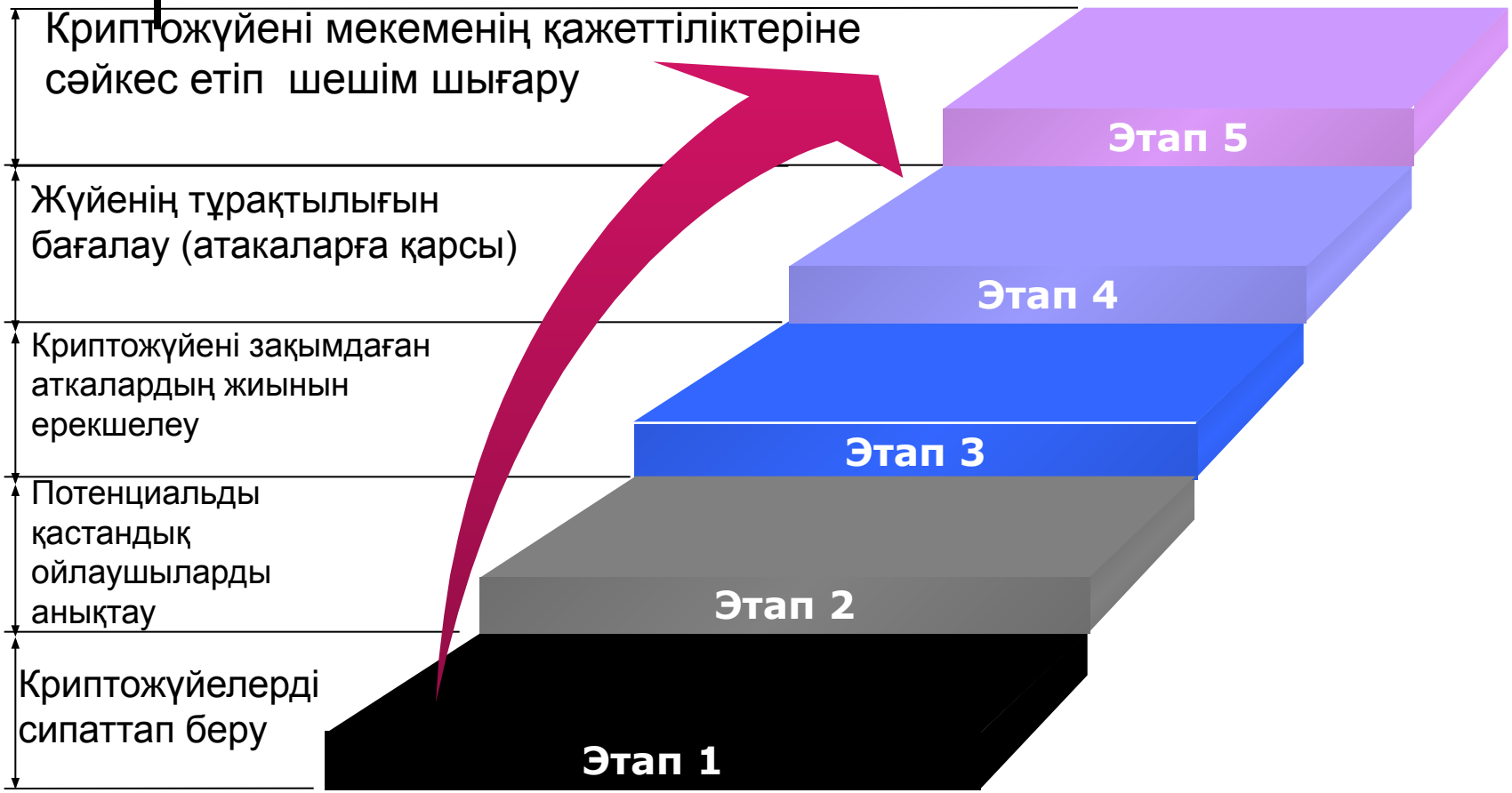
Салыстыру сараптамасы

Бағалау әдісі	Қолданылуы	Экономикалық көрсеткіші	Қастандық ойлаушының мүмкіндіктері
Криптотұрақтылықтың сараптамасы	+	-	±
Ойындар теориясы / В.П.Ивановтың Мат. моделі	±	+	-
Ақпараттық тәуекелдіктердің сараптамасы	-	+	+
Криптохаттамалардың сараптамасы	±	-	-

Мақсаттары мен міндеттері

- Берілген қолдану контекстіндегі криптожүйенің тиімділігін бағалайтын формальды модельді құру.
- Криптожүйелердің тұрақтылығын бағалайтын әр түрлі атакалардан қорғауға арналған инструментальды құралдарды құру.
- Ақпараттық қауіпсіздікті қамтамасыз етудегі инвестицияның экономикалық тиімділігінің әдісінің сараптамасын бағалау және жүйелендіру.

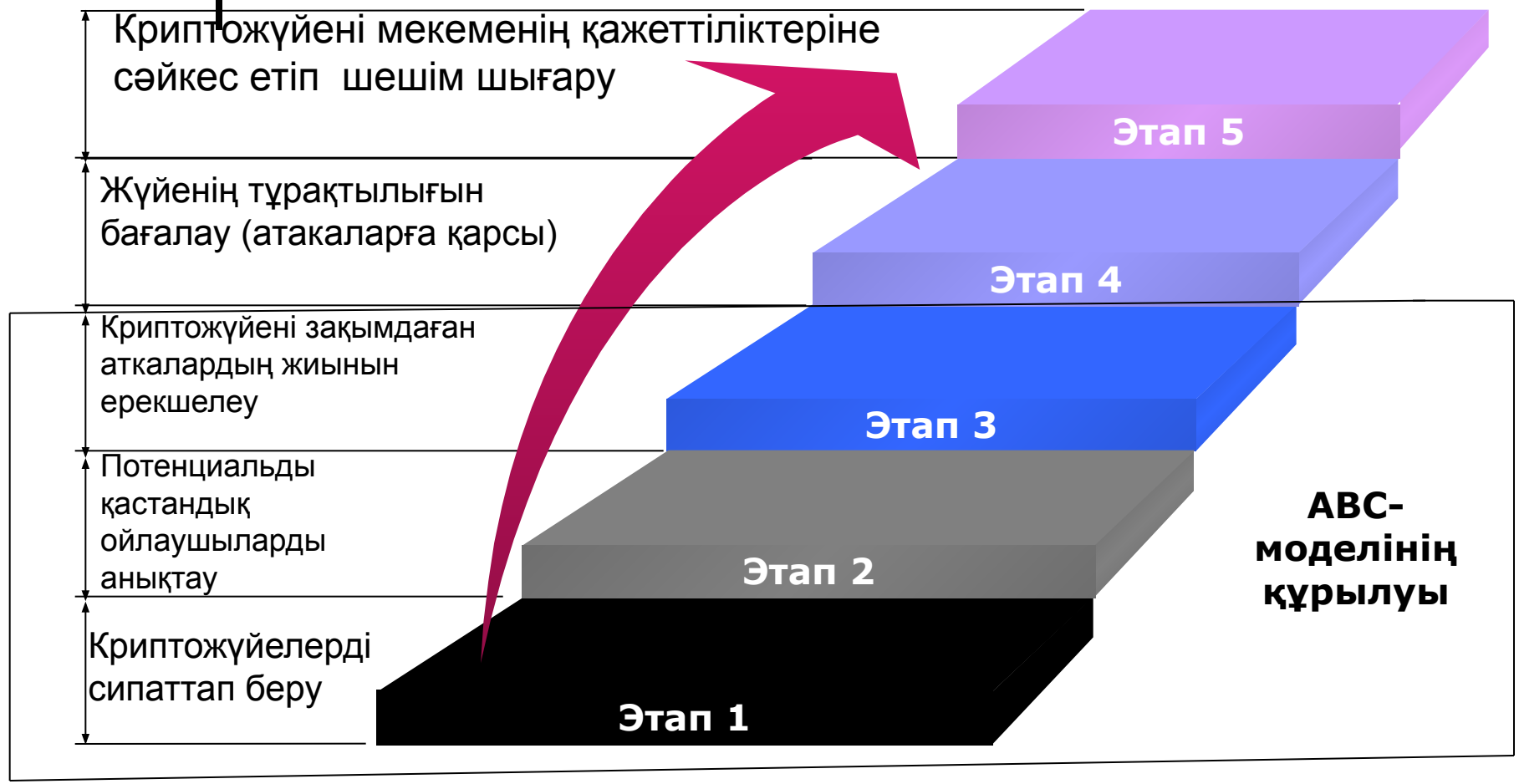
Криптожүйенің тиімділігін бағалау процесі



ABC - қауіп-қатер моделі

- “**A**” от **A***ttack*
- “**B**” от *code-***B***reaker*
- “**C**” от **C***ryptosystem*

Криптожүйенің тиімділігін бағалау үрдісі



Криптожүйелердің классификациясы

- **Ули Маурердың** классификациясы (Ueli Maurer) – кілттердің саны бойынша:
  - Кілтсіз
  - Біркілтті
  - Екікілтті
- **Жиля Брассардың** классификациясы (Gilles Brassard) - шифрлеу алгоритмінің құпиялығы бойынша:
  - Қолдануы шектеулі криптожүйелер
  - Жалпы қолданудағы криптожүйелер

Криптожүйелердің классификациясы

- **Криптоалгоритм туралы ақпараттың қол жетімділігі бойынша**
  - Қолдануы шектеулі криптожүйелер
  - Жалпы қолданудағы криптожүйелер
- **кілттердің саны бойынша:**
  - Кілтсіз
  - Біркілтті
  - Екікілтті
- **Криптоалгоритмнің тұрақтылығы бойынша**
  - Шартсыз тұрақты
  - Дәлелденген тұрақты
  - Шамалас тұрақты
- **Шифрлеу құралдарының қолданылуы бойынша**
  - Программалық
  - Аппараттық
  - Программа-аппараттық
- **Сертификатының бар болуы бойыншы**
  - Сертификатталған
  - Сертификатталмаған

Бұзушылардың классификациясы

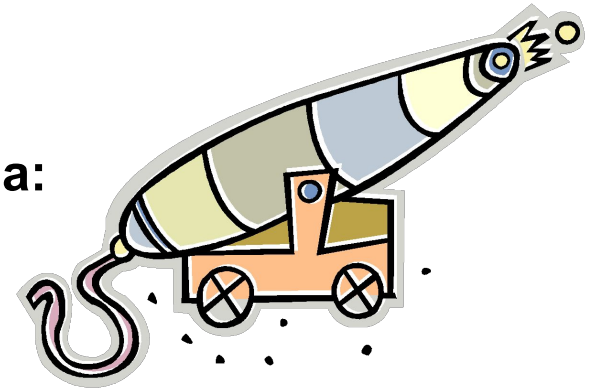
- **Бұзушының моделі төмендегілерді есептеуі міндетті:**
  - Адамдар категориясы, бұл категорияда бұзушы болуы мүмкін;
- Бұзушының біліктілігі және оның техникалық жабдықталуы туралы деректер;
  - Бұзушының орындалуы мүмкін болатын мақсаттары және одан күтетін іс-әрекет.
  - **Мотив (деректеме) бойынша Брюса Шнайердың классификациясы:**
  - Арнайы бұзуға ниеттенген бұзушылар;
  - Эмоциональды күйде бұзуға ниеттенген бұзушылар;
  - Достары/туысқандары;
  - Өндірістік бәсекелестері;
  - Пресса;
  - Үкімет;
  - Полиция;
  - Ғылыми-зерттеу мекемелері.

Бұзушылардың классификациясы

- **Техникалық жабдықталуы бойынша**
  - Дербес компьютер
  - ЭЕМ желісі
  - Суперкомпьютер
- **Соңғы мақсаты бойынша**
  - алгоритмде әлсіздікті анықтау (Обнаружение слабости в алгоритме)
  - Алгоритмді түгелімен бұзу
- **Шифрленетін құралдарға енуі бойынша**
  - «ішкі» бұзушы
  - «сыртқы» бұзушы
- **Дайындық деңгейі бойынша**
  - Қолданушы деңгейінде компьютермен өзара әрекеттестік
  - Математикалық аппарат
  - Программалау
  - Электротехника және физика
  - Әлеуметтік инженерия
- **шифрлеу туралы бірінші ақпарат бойынша**
  - қолданушы
  - криптограф
  - «клептограф»
- **кооперацияның мүмкіндігі бойынша**
  - «жалғыз»
  - Ұйым

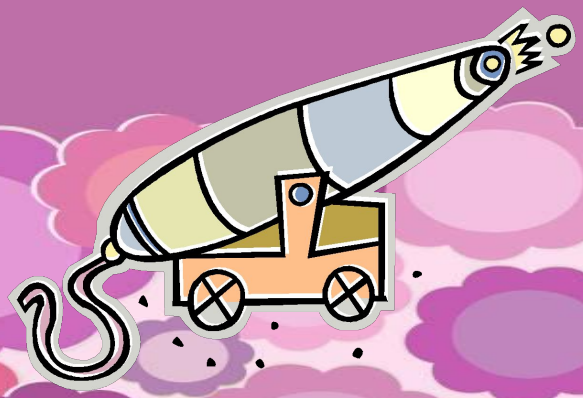
Шабуылдардың классификациясы (1/2)

- **Ашық және шифрленген мәтінге ену негізінде:**
  - тек шифрмәтін
  - Ашық мәтін
  - Таңдап алынған ашық мәтін
  - Адаптивті таңдап алынған ашық мәтін
  - каналдардан алынған ақпарат
- **Үрдістерді бақылауы бойынша:**
  - Пассивті
  - активті
- **Шабуылдардың шығуы бойынша:**
  - Толық бұзу
  - глобальды дедукция
  - Бөліктенген дедукция
  - Ақпараттық дедукция
- **критикалық ресурстары бойынша:**
  - жады
  - уақыт
  - Мәліметтер



Шабуылдардың классификациясы (2/2)

- **Әр түрлі шифрлерге қолданылуы бойынша**
  - универсальды (әмбебап)
  - шифрдың анықталған категориясы бойынша
  - нақты криптоалгоритмге
- **Қолданылатын құралдары бойынша**
  - Математикалық әдістер
  - шифрлеу үрдісінің физическалық параметрлерін алатын (перехват) құралдар
  - Эволюциялық программалау
  - Кванттық компьютерлер
- **Қадам бойынша**
  - Құпиялықтың бұзылуы
  - Бүтіндіктің бұзылуы
  - Қол жетімділіктің бұзылуы
  - **параллельдеу мүмкіндігі бойынша**
  - Бөлінген
  - Бөлінбеген



Классификациялар

- **Криптожүйенің классификациясы**

-криптоалгоритм туралы ақпараттың қол жетімділігі бойынша

-Кілттердің саны бойынша

- криптоалгоритмдің тұрақтылығы бойынша
- шифрлеу құралдарын қолдануы бойынша
- Сертификатының бар болуына байланысты

- **Бұзушылардың классификациясы**
  - техникалық жабдықталуы бойынша
  - Соңғы мақсаты бойынша

- шифрленетін құралдарға енуі бойынша
  - Дайындық деңгейі бойынша
  - по первичной информации о средстве шифрлеу құралдарының бірінші аақпараты бойынша
  - кооперацияның мүмкіндігі бойынша

- **шабуылдардың классификациясы**
  - ашық және шифрленген мәтінге енуі бойынша
  - үрдістерді бақылауы бойынша
  - Шабуылдың шығуы бойынша
  - критикалық ресурстар бойынша
  - әр түрлі шифрлерге қолданылу деңгейі бойынша
  - Қолданылатын құралдар бойынша
  - Қадам бойынша
  - параллельдеу мүмкіндігі бойынша

Экономикалық тиімділікті бағалау әдісін таңдау

Бағалау әдістері	Артықшылықтары	Кемшіліктері
Инвестицияларды қайтару коэффициенті (ROI)	Қаржыгерлерге түсінікті көрсеткіш	Ақиқатты есептеу әдістерінің жоқтығы «Статикалық» көрсеткіш
Меңгеру бағасы (TCO)	Тек шығындардың негізінде жобаны реализациялаудың бүтіндігін бағалауға мүмкіндік береді ЖЦ жүйесінің этапындағы шығындарды бағалауға мүмкіндік береді	Қауіпсіздік жүйесінің сапасын ескермейді «Статикалық» көрсеткіш АТ үшін мамандандырылған көрсеткіш
Инвестицияның тиімділігінің дисконтты көрсеткіштері	Қаржыгерлерге түсінікті көрсеткіш Уақытқа тәуелді қаржы құралдарын есептейді Жобаны реализациялауға байланысты қаржы құралдарын есептейді	Есептеудің қиындығы

Шешімдер

«As information security is about power and money …, the evaluator should not restrict herself to technical tools like cryptanalysis and information flow, but also apply economic tools»

Ross Anderson,
Professor in Security Engineering at the University of Cambridge Computer Laboratory

Тест сұрақтары

281. Қауіпсіздіктің функцияларына және оларды іске асыратын тетік көрсетілетін талаптар
282. Технологияға және өңдеу және пайдалануды процесс көрсетілетін талаптар
283. Қауіпсіздіктің бағасының объектінің тіршілік циклдасының бірінші кезеңі
284. Екінші қауіпсіздіктің бағасының объектінің тіршілік циклдасының кезеңі
285. Қауіпсіздіктің бағасының объектінің тіршілік циклдасының үшінші кезеңі
286. Қауіпсіздіктің бағасының объектінің тіршілік циклдасының төртінші кезеңі
287. Қауіптер келесі параметрлермен бейнеленеді
288. Қолдануға болатын параметрлері
289. Зақымдана алған параметрлер
290. Осал жерлер мынандай кемшіліктен пайда болады

Тест сұрақтары

291. ОК -ң функционалдық талаптарының сыныптары
292. Бүтіндікке талаптары және қауіпсіздіктің осы сервистері және іске асыратын олардың тетіктерінің бақылауына
293. Бұл сыныптың талаптары қауіпсіздіктің атрибуттармен және параметрлерімен басқаруларға жатады
294. Бағаның объектінің қауіпсіздік тиетін мәліметтердің анықталу, тіркеу, сақтау, талдауы
295. Ашылу және оның теңестіру мәліметтерінің қолдануынан қолданушының қорғауы
296. Қолданудың айғағының жасырып қалуы бар ақпараттық сервисін қолдану
297. Бұзылу немесе ақау туған жағдайда тіпті ақпараттық сервистердің ашықтығын сақтау
298. Қорлардың рұқсат етілмеген монополизациясынан (квоталардың тетіктің қолдануы жолымен) қорғау
299. Сервистерді қайтадан қолдану мүмкіндігі, бірақ қолданушылардың профильлерінің сипаттамаларын құрастырудан қорғайды
300. Объекттерге және/немесе басқа қолданушылар, субъекттерге әсер қолданушының идентификаторының