ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ТҰҢҒЫШ ПРЕЗИДЕНТІ - ЕЛБАСЫНЫҢ ҚОРЫ

«ҒЫЛЫМ ЖӘНЕ БІЛІМ – 2017»

студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ – 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«SCIENCE AND EDUCATION - 2017»

14th April 2017, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

«Ғылым және білім - 2017»
студенттер мен жас ғалымдардың
XII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XII Международной научной конференции
студентов и молодых ученых
«Наука и образование - 2017»

PROCEEDINGS
of the XII International Scientific Conference
for students and young scholars
«Science and education - 2017»

2017 жыл 14 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2017» студенттер мен жас ғалымдардың XII Халықаралық ғылыми конференциясы = The XII International Scientific Conference for students and young scholars «Science and education - 2017» = XII Международная научная конференция студентов и молодых ученых «Наука и образование - 2017». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2017. – 7466 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-827-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-827-6

Список использованных источников

1. Стругайло В.В. Обзор методов фильтрации и сегментации цифровых изображений // Наука и образование: научное издание МГТУ им. Н.Э. Баумана, № 05, 2012. – сс. 270 – 281.
2. Khairnar T., Harikiran, Chandgude A., Sivanantham S. Sivansankaran K. Image Edge Detection in FPGA // International Conference on Green Engineering and Technologies (IC-GET 2015). – Online Conference.
3. Chaple G., Daruwala R.D. Design of Sobel Operator based Image Edge Detection Algorithm on FPGA // International Conference on Communication and Signal Processing, India, 2014. – pp. 788-792.
4. Pawar P.H. Patil R.P. FPGA Implementation of Canny Edge Detection Algorithm // International Journal of Engineering And Computer Science, Volume 3, Issue 10, 2014. – pp. 8704-8709.
5. Shimpi H., Gaikwad N., Dhage M., Pawar A.S. Implementation of Edge Detection Algorithm Using FPGA // International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 4, 2015. – pp. 2193-2197.
6. Жуков К. Модельное проектирование встраиваемых систем в LabVIEW. – ДМК Пресс, 2011. – 688 с.
7. Mathworks, Simulink User's Guide. – The Mathworks Inc., Natick, MA, USA, 2016. – 3290 p.

ӘОЖ 004.056.53

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ҚАУІП-ҚАТЕРЛЕРІН БАҒАЛАУ ӘДІСТЕРІ

Адамжанов Тлек Болатханұлы
tlek86@mail.ru
Л.Н.Гумилев атындағы ЕҰУ «6М060200-Информатика» мамандығының 1 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – А.Сексенбаева

Есептеуіш техника құралдарының дамуы адамзат алдында ақыл-ой еңбегін автоматтандыру бойынша айтқысыз мүмкіндіктер ашты және кең көлемде әртүрлі автоматтандырылған ақпараттық және басқарушы жүйелерді жасауға алып келді. Осыған орай ақпаратты қорғау кез-келген компанияның маңызды, әрі басты міндеттерінің бірі болып табылады. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V Қазақстан Республикасының Заңына сәйкес ақпараттық қауіпсіздік бұл – электрондық ақпараттық ресурстардың, ақпараттық жүйелердің және ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалуының жай-күйі.

Ақпаратты қорғау құралдарын ақпараттық қауіпсіздіктің қауіп-қатерлеріне талдау мен бағалау жүргізілмейінше жобалауға, сатып алуға немесе орнатуға болмайды. Қауіп-қатерлерді бағалау процесінің басты мақсаты ақпараттық жүйелер мен оның ресурстарына (активтеріне) қатысты қауіп-қатерлердің сипаттамасын анықтау болып табылады. Алынған мәліметтер негізінде қажетті қорғау құралдары таңдалуы мүмкін. Қауіп-қатерлерді бағалау барысында қатерлердің және осалдылықтардың маңыздылығы, ақпараттық ресурстардың құндылығы, жоспарланған қорғау құралдарының тиімділігі сияқты факторлар ескеріледі.

Қауіп-қатер дегеніміз шығын немесе зиян әкелуі мүмкін жай-күй болып табылады. Қауіп-қатерді бағалау – шығынды немесе зиянды сандық немесе сапалық түрде анықтау үрдісі.

Қауіп-қатерді талдау барысында, болжалды зиян (қатер төнген жағдайда) қорғауға бағытталған шаралар мен құралдарға жұмсалған шығындармен салыстырылады. Бұдан кейін бағаланып жатқан қауіп-қатерге қатысты келесі шешімдер қабылданады:

– төмендету, мысалы қатерді іске асыру мүмкіндігін немесе қиратқыштық коэффициентін азайтатын қорғау құралдары мен мехнизмдерін еңгізу арқылы;

– қатерге бейім ресурсты қолданудан бас тарту арқылы жою;

– ауыстыру, мысалы, сақтандырылған, бұл ретте қауіпсіздік қауіп-қатерлері іске асатын болса, шығындарды ресурстың иесі емес, сақтандыру компаниясы көтеретін болады;

– қабылдау.

Қауіп-қатерді сәйкестендіру қауіп-қатер элементтерінің (қорғау объектілерінің, қатерлердің, осалдылықтардың) тізімі мен сипаттамасын құру болып табылады.

Қорғау объектілерінің келесі түрлерін атап өтуге болады: ақпараттық активтер; бағдарламалық жасақтама; физикалық активтер; сервистер; адамдар және олардың біліктілігі, дағдылары мен тәжірибелері; мекеменің беделі мен имиджі сияқты материалдық емес ресурстар. Әдетте, тәжірибеде бірінші үш топ қарастырылады. Қалған қорғау объектілері бағалауға қиын болғандықтан қарастырылмайды.

Қауіп-қатерлерді сәкестендіру кезеңінде қатерлерді және осалдылықтарды сәйкестендіру де жүргізіледі. Бұл үшін бастапқы деректер ретінде аудиттің нәтижелері, ақпараттық қауіпсіздік оқиғалары жайлы мәліметтер, пайдаланушылардың, ақпараттық қауіпсіздік бойынша мамандардың, ИТ-мамандардың және сыртқы кеңесшілердің сарапшылық бағалаулары қолданылады.

Ең қиыны шартты түрде келесі кезеңдерге бөлуге болатын қауіп-қатерді бағалау үдерісі болып табылады: қауіп-қатерді сәйкестендіру, қауіп-қатерді талдау, қауіп-қатерді бағалау.

Қауіп-қатерлерді сәйкестендіру кезеңінде алынған ақпарат қауіп-қатерлерді талдау үдерісінде мыналарды анықтау үшін қолданылады:

– активтердің қауіпсіздігін бұзу нәтижесінде мекемеге әсерін тигізетін ықтимал шығындарды;

– мұндай қауіпсіздікті бұзудың ықтималдылығын;

– қауіп-қатердің көлемін.

Ықтимал зиянның көлемі активтердің бағасы мен олардың қауіпсіздігін бұзу салдарының ауырпалығын есепке ала отырып құрылады.

Ықтимал зиянның мәнін қалыптастыратын екінші құраушы болып активтердің қауіпсіздігін бұзу салдарының ауыртпалығы табылады. Барлық ықтимал салдар және олардың мекемеге, серіктестеріне және қызметкерлерге теріс әсер ету дәрежесі есепке алынады.

Ақпараттық активтің құпиялық, тұтастық, қолжетімділік және басқа да маңызды қасиеттерін бұзу салдарының ауыртпалық дәрежесін анықтау қажет, ал содан кейін ортақ бағаны табу қажет.

Қауіп-қатерлерді талдаудың келесі кезеңі қатерлерді іске асыру мүмкіндігін анықтау болып табылады.

Ықтимал зиянның көлемі мен қатерлерді іске асыру мүмкіндігі анықталғаннан кейін қауіп-қатердің көлемі анықталады. Қауіп-қатерлерді анықтау активтердің қауіпсіздігін бұзудың ықтимал салдарын білдіретін ықтимал зияннан және қатерлерді жүзеге асыру мүмкіндігінен құрылады. Мұндай анықтау жиі матрица арқылы іске асады, мұндағы жолдарда зиянның ықтимал мәні, ал бағандарда қатерлерді жүзеге асыру мумкіндігі орналасады.

Әрі қарай қауіп-қатердің есептеу деңгейлері қауіп-қатер деңгейінің шкаласымен салыстырылады. Бұл анықталған қауіп-қатерлердің мекеме бизнесіне әсерін нақты бағалау үшін және қауіп-қатер деңгейлерінің мәнін басшылыққа жеткізу үшін қажет. Сонымен қатар қауіп-қатерлерді бағалау әрі қарай іс-әрекетті қажет етпейтін қауіп-қатердің жарамды деңгейлерін сәйкестендіруі қажет. Қалған барлық қауіп-қатерлер қосымша шаралар қолдануды қажет етеді.

Қауіп-қатерлерді бағалау нәтижелері қауіп-қатерлерді өңдеу іс-шараларының артықшылығы мен экономикалық тиімділігін анықтау үшін қолданылады, қауіп-қатерлер деңгейін төмендететін қорғау шараларын таңдау бойынша дәйекті шешім қабылдауға

мүмкіндік береді.

Заманауи басқару жүйесі ақпараттық қауіпсіздіктің ықтимал қауіп-қатерлерін бағалаусыз жүзеге аспайды. Қазыргі кезде қауіп-қатерді бағалаудың бірнеше әдістері бар. Солардың кейбірі төменде көрсетліген:

– CRAMM – Ұлыбританияда қолданылатын қауіп-қатерлерді талдау және басқару әдісі;
– OCTAVE – мекемелерде қауіп-қатерлерді бағалау әдісі;
– ГРИФ әдісі;
– RiskWatch – қауіп-қатерлерді талдау әдісі және бағдарламалық құралдар жиыны;
– CORAS әдісі;
– ISO/IEC 27005:2011 – ақпараттық қауіпсіздіктің қауіп-қатерлер менеджменті халықаралық стандарты;
– MSAT – қауіп-қатерлерді Microsoft әдісіне сәйкес бағалау.

CRAMM әдісінің негізінде талдаудың сандық және сапалық әдістерін қамтитын қауіп-қатерлерді бағалаудың кешенді тәсілі жатыр. Әдіс әмбебап болғандықтан, ірі әрі шағын мекемелерге, үкіметтік әрі коммерциялық секторларға сай келе береді. Әртүрлі мекемелер түрлеріне арналған CRAMM бағадарламалық жасақтамасы бір-бірінен өзінің білім қорымен ерекшеленеді. Коммерциялық мекемелер үшін коммерциялық профиль, ал үкіметтік мекемелерге арналған үкіметтік профилі бар. Үкіметтік профиль американдық ITSEC стандартының талаптарына сай аудит жүргізуге де мүмкіндік береді.

CRAMM әдісі бизнес-процестерді сипаттайтын немесе қауіп-қатерлерді бағалау процессі жүргізілгені жайлы есептеме сияқты құжаттарды есепке алмайды. Қауіп-қатерлермен жұмыс істеу стратегиясына қатысты CRAMM тек оларды төмендету әдісін ғана қолданады. Қауіп-қатерлерді басқарудың ауыстыру немесе қабылдау сияқты әдістері қарастырылмайды. Сонымен қатар әдісте келесілер қарастырылмаған: басқару тәсілдерін біріктіру үрдісі және әрбір тәсілдің міндеттері; басқару тәсілдерінің қолдану тиімділігін бақылау және қалдық қауіп-қатерлерді басқару тәсілдері; қауіп-қатерлердің максималды мүмкін болған көлемін қайта есептеу; оқиғаларға жауап қайтару үрдісі.

CRAMM-ді практикалық қолдану жоғары білікті мамандарды тартумен, еңбек сыйымдылығы және қауіп-қатерлерді бағалау үрдісінің ұзақтылығымен ерекшеленеді. Сонымен бірге лицензия бағасының қымбат екенін айта кету керек.

OCTAVE әдісінің ерекшелігі – ол сырттан кеңесші жалдамай-ақ, барлық талдау үрдісін мекеме қызметкерлерінің күшімен жүзеге асыруға болады. Ол үшін бизнестің қауіпсіздік саласындағы ықтимал оқиғалардың әсерін жан-жақты бағалауға және оған қарсы әрекеттерді ойлап табуға мүмкіндік беретін техникалық мамандар мен әртүрлі деңгейдегі басшылардан тұратын аралас топ құрылады.

OCTAVE талдаудың үш фазасын есекереді:
– активпен байланысты қатерлер профилін жасауды;
– инфрақұрылымдық осалдылықтарды сәйкестендіруді;
– қауіпсіздіктің стратегиясы мен жоспарын құруды.

Қатер профилі активке сілтемені, активке қолжетімділік түрін, қатер көздерін, бұзушылық түрлерін немесе мотивті, ортақ қолжетімді каталогтарда қатерлердің сипаттамаларына сілтемелер мен нәтижені қамтиды. Қатерлер шығу түріне байланысты келесі түрлерге бөлінеді:

– мәліметтерді табыстау желісі арқылы іске асатын және бұзық адам тарапынан келетін қатерлер;
– физикалық қолжетімділікті пайдаланатын бұзық адам тарапынан келетін қатерлер;
– жүйе жұмысындағы ағаттықпен байланысты қатерлер;
– басқалары.

Нәтижесі ақпараттық ресурсты ашып көрсету, өзгерту, жоғалту немесе қирату болуы мүмкін немесе қосылымды үзу болуы мүмкін. Қызмет көрсетпуі мүмкін.

ГРИФ әдісі қауіп-қатерді бағалаудың сандық және сапалық әдістерін қолданады, сондай-ақ соңғы әдістің компаниямен қабылдау шарттарын анықтайды және қауіпсіздік шараларын еңгізуге арналған инвестициялардың қайтарылу есебін өз ішіне қамтиды. ГРИФ қауіп-қатерлерді талдайтын басқа әдістерден қауіп-қатерлерді төмендетудің барлық тәсілдерін (ауыстыру, төмендету және қабылдау) ұсынуымен ерекшеленеді. Бұл әдіс бизнес-процестерді сипаттайтын немесе ақпараттық қауіпсіздіктің қауіп-қатерлерін бағалау процессі жүргізілгені жайлы есептеме сияқты құжаттарды есепке алады.

RiskWatch әдісі қауіп-қатерді бағалаудың сандық және сапалық тәсілдерін қолданады. Бұл әдісті қолдану арқылы қауіп-қатерлерді талдау жұмыстары салыстырмалы түрде күрделі емес. Мұндай әдіс ұйымдастырушылық және әкімшілік факторларды есепке алмай, қорғаудың бағдарламалық-техникалық деңгейінде қауіп-қатерлерге талдау жүргізу керек болған кезде қолданылады. RiskWatch-тың елеулі артықшылығы болып интуитивті интерфейсі мен жаңа категориялар, сипаттамалар, сұрақтар және т.б. еңгізу мүмкіндігі бар әдістің зор икемділігі табылады.

CORAS «Ақпараттық қауіпсіздік саласындағы қызметкерлердің хабардарлығын көтеру бағдарламасы» сияқты қауіп-қатерлерді басқару бойынша тиімді шараларды қарастырмайды. Мұндай бағадрлама ақпараттық қауіпсіздік саласындағы корпоративті талаптар мен ақпараттық жүйелерді қауіпсіз қолдану ережелерін білмеу себебінен туындаған компания қызметкерлерінің ақпараттық қауіпсіздік режимін бұзумен байланысты ақпараттық қауіпсіздіктің қауіп-қатерлерін төмендетуге мүмкіндік береді. Сонымен бірге CORAS-та қауіп-қатерлерді бағалау мерзімі мен олардың мөлшерін жаңарту қарастырылмаған. Бұл әдістің бір реттік бағалау жасауға ғана жарамды екенін және әрдайым қолдануға келмейтінін көрсетеді.

CORAS-тың артықшылығы – бұл әдісті іске асыратын бағдарламалық өнім тегін және орнату үшін және қолдану үшін айтарлықтай ресурстарды талап етпейді.

ISO/IEC 27005:2011 – ақпараттық қауіпсіздіктің қауіп-қатерлер менеджменті халықаралық стандарты әсіресе ISO/IEC 27001 сәйкес ақпараттық қауіпсіздік менеджмент жүйесінің (АҚМЖ) талаптарын ұстана отырып, мекемеде ақпараттық қауіпсіздік қауіп-қатерлерін басқару бойынша ұсыныстармен қамтамасыз етеді. Бірақ бұл халықаралық стандарт ақпараттық қауіпсіздіктің қауіп-қатерлерін басқару бойынша белгілі бір әдістерді ұсынбайды. Бұл стандарт мекемеде, мысалы, АҚМЖ жүзеге асу саласына, қауіп-қатерлер менеджментін пайдалану саласына немесе өнеркәсіп секторына байланысты қауіп-қатерлерді басқару тәсілін анықтау үшін арналған. Көптеген әдістер АҚМЖ талаптарын орындау үшін осы халықаралық стандартта сипатталған құрылымды қолдана алады.

Microsoft әдісінің маңызды көрсеткіштері: бизнеске арналған профиль (бизнес ортаға байланысты қауіп-қатердің өзгеру көлемі, әртүрлі салада жұмыс атқаратын мекемелердегі жүйенің қорғаныс деңгейін анықтау барысында әрдайым есепке алынбайтын шынымен де маңызды параметр) және эшелондалған қорғаныстың индексі (қорғаныс деңгейінің жиынтық көлемі) болып табылады. MSAT қауіп-қатерлер деңгейінің сандық бағалауын бермейді, бірақ сапалық бағалау дәрежелік шкалаға байланысты болуы мүмкін.

MSAT қауіпсіздік шараларын еңгізуге жұмсалған инвестициялардың тиімділігін анықтауға мүмкіндік береді, бірақ ақпараттық активтерді алдын алуға, анықтауға, түзетуге және қалпына келтіруге бағытталған шаралар арасында тиімді баланс табуға мүмкіндік бермейді.

Қорытындылай келе, жоғарыда аталған әдістердің ішінен CORAS әдісі орта көлемді компаниялардағы қауіп-қатерлердің деңгейін анықтауға арналған бір реттік бағалау жүргізуге ең тиімді болып табылады. Егер ақпараттық қауіпсіздіктің қауіп-қатерлерін ішкі қызметкерлердің көмегімен бағалау талабы тұрса, онда OCTAVE әдісін қолданған жөн. Техникалық деңгейде жүйелі түрде бағалау жүргізілетін қауіп-қатерлерді басқару үшін CRAMM әдісі лайқты. Microsoft Security Assessment Tool және RiskWatch әдістері ақпараттық қауіпсіздік қауіп-қатерлерін басқаруда үнемі бағалау жүргізуді қажет ететін және оларды төмендету бойынша дәйекті шаралар жоспарын құруды талап ететін алып

компанияларда қолданылғаны дұрыс.

Қолданылған әдебиеттер тізімі

1. «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы Қазақстан Республикасының Заңы.
2. Галатенко В.А. Основы информационной безопасности: учебное пособие. – М.: Интернет-Университет Информационных Технологий, 2008, 205 с.
3. Международный стандарт ISO/IEC 27005:2011. Информационная технология –Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности BS ISO/IEC 27005:2011.
4. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии, 2015, № 1(9). С. 73–79.
5. http://www.intuit.ru/studies/courses/531/387/lecture/8996?page=1#sect2

ӘОЖ 625.7

ИНТЕЛЛЕКТУАЛДЫ КӨЛІК ЖҮЙЕСІНІҢ ЖОБАСЫН ӨҢДЕУ ПРОЦЕСІН ЗЕРТТЕУ

Азат Жанар
janar-azat@mail.ru
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің МЕТБҚ-21 тобының магистранты, Астана, Қазақстан
Ғылыми жетекшісі – т.ғ.к., доцент Жумадиллаева А.К.

Көлік жүйесін жобалау кезінде орындалатын негізгі бағыттар мен тапсырмалар, негіздеу, енгізу және жетілдіру кезеңдеріндегі интеллектуалды көлік жүйесінің аумақтық жобасын жасау шарттары қарастырылған. Сонымен қатар, интеллектуалды көлік жүйесінің аумақтық жобасын жобалау тұжырымдамасы қарастырылған және әрбір аумақтық жобаны бөлек қарастыру негіздемесі берілген және әрбір үшін жеке тиімділік индикаторының матрицасын өңдеу жасалады. Сәйкесінше, аумақтық жобалардың функционалды архитектурасын жасау шарттары анықталған. Мақаладаинтеллектуалды көлік жүйесінің құрылымы бірнеше өзара тәуелді деңгейлердің жиынтығы ретінде қарастырылады: технологиялық, техникалық шешімдер және психофизиологияның деңгейлері, сонымен қатар олардың сипаттамасы берілген. Және де эксперименталды зерттеулерде жүргізілген нәтижелер келтірілген. Бұл зерттеудің мақсаты қарастырылатын өзара тәуелді деңгейлердің алуан түрлерін зерттеу және интеллектуалды көлік жүйесінің оптималды аумақтық жобасының идеологиясын анықтау болып табылады. Бұл мақаланың негізгі қорытындысы енгізілетін интеллектуалды көлік жүйесінің жоғары тиімділігін қамтамасыз ету үшін ұсыныстар мен шарттар жиынтығын анықтау болып табылады.

Интеллектуалды көлік жүйесінің аумақтық жобасын өңдеу және қалыптастырудың алғашқы кезеңінде өмірлік цикл бойына тиімді жүйе жасау үшін болжалды тиімділіктің расталған бағасы, капиталды және эксплуатациялық шығындар маңызды болып табылады. Интеллектуалды көлік жүйесінің аумақтық жобасын өңдеу кезеңінде тапсырыс беруші шешім қабылдауының ең таралған әдісі тиімді жобаның ең кіші бағасы таңдауда негізделген. Тез дамушы технологиялық ортаның шартында интеллектуалды көлік жүйесі жобасын енгізу мен пайдалану тәжірибесін қарастыра отырып, тәжірибеде негізделген тапсырыс берушінің шешімін және типтік техникалық шешімдерді қабылдау алғашында ескірген және тиімсіздеу жүйе жасалған. Максималды тиімділік пен жүйе әсерін өзгертуді жобалауда негізделген интеллектуалды көлік жүйесінің оптималды аумақтық жобасында тапсырыс беруші таңдауы қарастырылып отырған салада қаржылық және техникалық саясатына сай құруға мүмкіндік береді.

Тиімділік индикатор матрицасы. Қарастырылып отырған интеллектуалды көлік