ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

С.А. Адилжанова

КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН АДАПТИВТІ БАСҚАРУҒА АРНАЛҒАН ЗАМАНАУИ ТӘСІЛДЕР МЕН ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

Монография

Алматы
«Қазақ университеті»
2025

ӘОЖ 004.056
КБЖ 32.973
А 25

Баспаға әл-Фараби атындағы Қазақ ұлттық университетінің Ғылыми кеңесінің шешімімен ұсынылған (№1 хаттама «29» қыркүйек 2025 ж.)

Рецензенттер:
Абай атындағы Қазақ ұлттық педагогикалық университеті,
техника ғылымдарының докторы, профессор
Б.С. Ахметов
әл-Фараби атындағы Қазақ ұлттық университеті,
физика-математика ғылымдарының кандидаты, профессор
Ш.Ж. Мусиралиева

Адилжанова С.А.

А 25 Киберқауіпсіздік ресурстарын адаптивті басқаруға арналған заманауи тәсілдер мен цифрлық технологиялар: монография / С.А. Адилжанова. – Алматы: Қазақ университеті, 2025. – 162 б.

ISBN 978-601-04-7297-6

Бұл монография киберқауіпсіздік ресурстарын адаптивті басқарудың теориялық және практикалық негіздерін талдауға арналған. Халықаралық стандарттар (ISO/IEC 27001, ISO/IEC TR 13335) негізінде ақпараттық-коммуникациялық жүйелердің қауіпсіздік модельдері қарастырылған. Ақпараттандыру объектілерінде ресурстарды бөлу есептері көп критерийлі шешім қабылдау мен ойын әдістері арқылы зерттелген. Генетикалық алгоритм негізінде ақпаратты қорғау құралдарын оңтайландыру тәсілдері ұсынылған. IIoT және цифрлық егіздер жүйелеріндегі киберқауіпсіздік мәселелері талданған. Жаңа әдіс ретінде модификацияланған генетикалық алгоритм енгізіліп, шешім қабылдауды қолдау жүйесінің прототипі әзірленген. Зерттеу нәтижелері мемлекеттік органдар, банк және телекоммуникация секторында қолдануға ұсынылады. Монографияның ғылыми жаңалығы – ресурстарды тиімді бөлу үлгілерін қалыптастыруында, ал практикалық маңызы – ұлттық инфрақұрылымның тұрақтылығы мен қауіпсіздігін арттыруында.

ӘОЖ 004.056
КБЖ 32.973

ISBN 978-601-04-7297-6

МАЗМҰНЫ

ҚЫСҚАРТЫЛҒАН СӨЗДЕР МЕН ТЕРМИНДЕР ТІЗІМІ

Қысқартылған сөз	Толық атауы / Түсіндірме
АКЖ	Ақпараттық-коммуникациялық жүйелер
IIoT	Industrial Internet of Things (өндірістік Интернет заттар)
LSTM	Long Short-Term Memory (ұзақ қысқа мерзімді есте сақтау нейрондық желісі)
CNN	Convolutional Neural Network (салынатын нейрондық желі)
CNN-LSTM	Convolutional Neural Network + LSTM (салынатын нейрондық желі + ұзақ қысқа мерзімді есте сақтау нейрондық желісі)
RBAC	Role-Based Access Control (рөлге негізделген қол жеткізуді басқару жүйесі)
TLS/SSL	Transport Layer Security / Secure Sockets Layer (қорғалған байланыс протоколдары)
IDS	Intrusion Detection System (басып кіруді анықтау жүйесі)
IDPS	Intrusion Detection and Prevention System (басып кіруді анықтау және болдырмау жүйесі)
AI	Artificial Intelligence (жасанды интеллект
ML	Machine Learning (машиналық оқыту)
MQTT	Message Queuing Telemetry Transport (телеметриялық хабарлар кезегі протоколы)
DoS	Denial of Service (қызмет көрсетуден бас тарту шабуылы)

Қысқартылған сөз	Толық атауы / Түсіндірме
XSS	Cross-Site Scripting (сайттар арасындағы скрипт шабуылы)
CSRF	Cross-Site Request Forgery (сайттар арасындағы өтінішті жалғандандыру)
CIP	Critical Infrastructure Protection (сындарлы инфрақұрылымды қорғау)
ОҚҚЖ	Оңтайлы Қолданбалы Қабылдау Жүйесі (Decision Support System)
GA	Genetic Algorithm (генетикалық алгоритм)
ШБӘ	Шешім қабылдауды бағалау (Decision Evaluation)
KZ-CERT	Қазақстан Республикасының Компьютерлік Инциденттерді Тіркеу Орталығы
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission (Халықаралық стандарттау және электротехника комиссиясы)
ISO/IEC TR 13335	Ақпараттық қауіпсіздікті басқару стандарттарына арналған техникалық есеп
ISO/IEC 27001	Ақпараттық қауіпсіздік басқару жүйелерінің халықаралық стандарты
SSADM	Structured Systems Analysis and Design Method (құрылымдық жүйелерді талдау және жобалау әдісі)
eGov	Electronic Government (электронды үкімет)
eHealth	Electronic Health (электрондық денсаулық сақтау жүйесі)

КІРІСПЕ

Қазіргі өркениет дамуында ақпараттық-коммуникациялық технологиялардың қарқынды өсуі адамзаттың барлық салаларына – мемлекеттік басқарудан бастап жеке тұлғалардың күнделікті өміріне дейін – елеулі ықпал етіп отыр. Әсіресе соңғы онжылдықта цифрландыру үдерісі тек дамыған мемлекеттерде ғана емес, дамушы елдерде де әлеуметтік-экономикалық өзгерістердің негізгі факторына айналды. Қазақстан да бұл процестен тыс қалған жоқ. Елдің стратегиялық құжаттарында цифрлық трансформацияны жеделдету ұлттық басымдық ретінде қарастырылып, электронды үкімет (eGov) платформасының жетілдірілуі, цифрлық банкинг пен қаржылық технологиялардың енгізілуі, денсаулық сақтау саласында eHealth жүйелерінің құрылуы және өндірістік секторда IIoT (Industrial Internet of Things) элементтерінің пайдаланылуы кең көлемде қолға алынуда. Осындай серпінді даму, сөзсіз, жаңа мүмкіндіктермен қатар, жаңа қауіптерді де тудырады. Қазақстанның цифрлық кеңістігінің кеңеюімен бірге елдің ақпараттық тәуелділігі де артып отыр. Егер бұрын ақпараттық жүйелерді бұзу тек жекелеген техникалық сипаттағы проблемалар ретінде қарастырылса, қазіргі жағдайда киберқауіпсіздік бүкіл мемлекеттің тұрақты дамуы мен ұлттық қауіпсіздігінің құрамдас бөлігіне айналды. Кибершабуылдардың экономикалық, әлеуметтік және саяси салдары барған сайын ауырлап, мемлекеттік органдардың, қаржы институттарының, білім беру және денсаулық сақтау жүйелерінің қалыпты қызметіне айтарлықтай зиян келтіруде.

Қазақстан Республикасының KZ-CERT компьютерлік инциденттерге әрекет ету қызметінің ресми деректеріне сүйенсек, соңғы жылдары жағдай төмендегі кестеде көрсетілгендей өзгерді:

Жыл	**Тіркелген оқиғалар саны**	**Ең жиі кездескен шабуыл түрлері**	**Дереккөз**
2023	~45 000	Фишинг, зиянды ПО, деректердің таралуы	KZ-CERT
2024	~82 000	Ботнет, трояндар, DDoS, фишинг	KZ-CERT (жылдық есеп)
2025 (қаңтар–мамыр)	30 000+	Ботнет, деректердің заңсыз таралуы, зиянды қосымшалар	KZ-CERT (оперативтік деректер)

Көріп отырғанымыздай, кибершабуылдардың қарқыны жыл сайын күшейіп, олардың салдары қоғамның әлеуметтік-экономикалық дамуына айтарлықтай әсерін тигізіп отыр. Қазақстан Республикасының KZ-CERT қызметінің деректеріне сәйкес, 2023 жылы шамамен 45 мың, 2024 жылы 82 мыңға жуық инцидент тіркелген. 2025 жылдың алғашқы бес айында ғана 30 мыңнан астам оқиға анықталды. Егер бұл үрдіс сақталса, жыл соңында көрсеткіш 100 мыңнан асуы ықтимал. Негізгі қауіптер қатарына фишинг, ботнет, деректердің заңсыз жариялануы, зиянды бағдарламалар және DDoS-шабуылдар жатады

Кибершабуылдардың түрлері әр алуан: фишингтік науқандар, зиянды бағдарламалар арқылы ақпарат ұрлау, қызмет көрсетуді тоқтату мақсатындағы DDoS-шабуылдар, ботнеттерді пайдалану арқылы жасалған қасқүнемдік әрекеттер және азаматтардың жеке деректерін заңсыз жариялау. Мәселен, 2024 жылы 2 миллионнан астам қазақстандықтың төлқұжат деректері интернеттің ашық сегментінде таралған оқиға қоғамда үлкен резонанс тудырды. Мұндай жағдайлар жеке тұлғалардың ғана емес, сонымен қатар мемлекеттік билік институттарының, ұлттық компаниялардың және банк секторының да сенімділігіне нұқсан келтіреді.

Әлемдік контекстке көз жүгіртсек, киберқауіптердің ауқымы әлдеқайда күрделі екені байқалады. Халықаралық ұйымдардың (IBM Security, Gartner, Check Point, Kaspersky Lab) соңғы жылдардағы сараптамалық есептеріне сәйкес, 2023–2024 жылдары кибершабуылдардың әлемдік экономикаға келтірген жылдық шығыны шамамен 8 триллион АҚШ долларын құраған. Бұл көрсеткіштің өзі-ақ киберқауіпсіздіктің бүгінгі таңда тек техникалық сала емес, ұлттық қауіпсіздік пен жаһандық экономикалық тұрақтылық мәселесі екенін айқын дәлелдейді.

Қазақстан үшін де мұндай жаһандық үрдістерден оқшау қалу мүмкін емес. Қаржы жүйесі, телекоммуникациялық инфрақұрылым және мемлекеттік басқару секторлары кибершабуылдардың басты нысанасына айналып келеді. Егер бұл бағытта тиімді алдын алу шаралары уақытылы қабылданбаса, елдің әлеуметтік-экономикалық дамуына айтарлықтай кедергі келтіруі мүмкін. Осыған орай, Қазақстанда соңғы жылдары бірнеше стратегиялық құжаттар қабылданып, жүзеге асырылуда. Соның ішінде «Қазақстанның киберқалқаны – 2022» тұжырымдамасы киберқауіпсіздік

жүйесін нығайтудың алғашқы қадамдарының бірі болды. Ал 2023–2027 жылдарға арналған Цифрландыру стратегиясында ақпараттық қауіпсіздік мәселесіне арнайы бөлім бөлініп, ұлттық деректерді қорғау, мемлекеттік органдардың ақпараттық жүйелерін күшейту, сондай-ақ киберқауіпсіздік саласында мамандар даярлау мәселелері кешенді түрде қарастырылған. Алайда аталған құжаттардың орындалуы барысында жиналған статистикалық деректер қауіп-қатерлердің азаймай, керісінше күшейіп отырғанын көрсетуде. Бұл жағдай киберқауіпсіздік саласында қолданылып жүрген тәсілдерді жетілдіру қажеттілігін айқындайды.

Ғылыми зерттеулер тұрғысынан алғанда, Қазақстанда киберқауіпсіздік тақырыбында жарияланған еңбектердің басым бөлігі техникалық шешімдерді сипаттаумен шектелген. Жүйелік деңгейде ресурстарды оңтайлы бөлу, көп критерийлі шешім қабылдау әдістерін енгізу, адаптивті басқару тетіктерін қолдану және эволюциялық есептеу әдістері (генетикалық алгоритмдер және т.б.) негізінде күрделі модельдерді қалыптастыру бағыттары толыққанды зерттелмеген. Бұл жағдай зерттеу тақырыбының ғылыми жаңалығын көрсетеді. Ұсынылып отырған ғылыми жұмыстың негізгі мақсаты – киберқауіпсіздік ресурстарын тиімді басқарудың әдістемелік негіздерін қалыптастыру және көп контурлы қорғаныс жүйелерінде оларды оңтайлы бөлу тәсілдерін әзірлеу болып табылады. Зерттеу мақсатына сәйкес мынадай міндеттер айқындалды: халықаралық стандарттар (ISO/IEC 27001, ISO/IEC TR 13335 және т.б.) негізінде ақпараттық-коммуникациялық жүйелердің қауіпсіздігін басқару модельдерін талдау; ақпараттандыру объектілерін қорғау үшін «объект – қауіп – қорғау» тұжырымдамасы мен көп деңгейлі «кибернетикалық кеңістік – коммуникациялық орта – физикалық кеңістік» моделін салыстырмалы тұрғыдан зерттеу; қолданыстағы ақпаратты қорғау құралдары мен экономикалық ұтымдылық модельдерін (Гордон-Леб, К.Задираки, Глушак-Новиков үлгілері) бағалау; көп критерийлі шешім қабылдау теориясы мен адаптивті басқару әдістерін қолдана отырып, ресурстарды бөлу есебінің математикалық моделін құру; сондай-ақ генетикалық алгоритмдер негізінде оңтайландыру тәсілін бейімдеп, шешім қабылдауды қолдау жүйесінің прототипін әзірлеу. Жүргізілетін зерттеу жұмысының теориялық маңыздылығы – киберқауіпсіздік жүйелеріндегі ресурстарды тиімді басқаруға арналған жаңа модельдер ұсынуда.

Ал практикалық құндылығы – алынған нәтижелерді мемлекеттік органдардың ақпараттық жүйелерінде, банк және телекоммуникация секторында, сондай-ақ стратегиялық инфрақұрылымда киберқауіпсіздікті арттыру мақсатында қолдануға болатындығында. Ресурстарды басқаруды модельдеу саласындағы ғылыми жұмыстарды талдау ақпаратты қорғау тараптары негізгі күш-жігердің қорғауға салынған инвестициялар көлемін анықтауға бағытталғанын көрсетеді. Бұл инвестицияларды қорғау объектілері арасында бөлу есеплері жекелеген зерттеулерге арналған. Сонымен қатар, қолданыстағы әзірлемелер шабуылдаушының ықтимал әрекеттері мен олардың салдарының ақпараттандыру объектісіндегі ақпараттық жүйе көрсеткіштері мен сипаттамаларының өзгеруіне әсерін сирек ескереді. Шабуылдар санының өсуі жағдайында шаруашылық қызмет субъектілерінің ақпаратын қорғауға бөлінетін шектеулі қаржы ресурстарын тиімді пайдалану есебі барған сайын маңызды бола түсуде және кез келген мемлекеттің ақпараттық қауіпсіздік және киберқауіпсіздік деңгейін айтарлықтай дәрежеде айқындайды. Сонымен қатар, белгісіздікте шабуылдаушы тараптың әрекеттерінің дәйектілігі алдын-ала белгісіз және белгілі бір ықтималдықпен мақсатты шабуыл сценарийін болжауға болған кезде, теориялық және ойын әдістерін қолдану және қарама-қайшылық жағдайларының өзгеру адаптивтілігін ескере отырып, ақпараттық қауіпсіздік объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу ақпараттық ресурстардың ағып кетуінен қаржылық шығындарды ең аз шамаға дейін азайтуға мүмкіндік береді. Ақпаратты қорғау құралдары құнының өсуі қорғау ресурстарын ұтымды пайдалану проблемасын өзектендіреді. Шешімдерді іздеу барысында уақыт өте келе шабуылдаушы тараппен қарсыласу жағдайларының өзгеруін ескеру қажет. Бұл ақпараттық ресурстардың «ескіруіне», олардың жаңаруына, жаңа шабуыл құралдарының пайда болуына, ақпаратты қорғау құралдары модернизациясына және т.б. байланысты. Нәтижесінде біз күрделі қорғаныс құрылымдарындағы ресурстарды адаптивті басқару есебін шешу қажеттілігіне келеміз.

Ақпараттандыру объектісі ақпараттық инфрақұрылымын талдау, ақпараттық қауіпсіздік және киберқауіпсіздік бағалау мен басқарудың кез келген әдістемесінің есепті кезеңі. Бұл талдау неғұрлым терең болса, бағалау нәтижесі соғұрлым объективті болады.

Осылайша, тиімді ақпаратты қорғау құралдары құру үшін кешенді түрде оның тиімділігін анықтайтын көрсеткіштердің жеткілікті үлкен санын ескеру қажет. Сонымен бірге, олардың талаптарының сәйкес келмеуіне байланысты әртүрлі көрсеткіштердің ұтымды мәндеріне қол жеткізу өте қиын және көбіне мүмкін емес. Нәтижесінде біз көп критерийлі есепке келеміз. Мұндай есепті шешу әрқашан да жеке көрсеткіштерге қойылатын талаптарды орындаудағы келісімге келу болып табылады. Мұндай көп критерийлі есептерді шешкен кезде әрдайым шешім алгоритмдерін таңдау дилеммасы пайда болады. Бұл, әсіресе, ақпаратты қорғауға байланысты есептерді қатысты, өйткені қорғау тарапының әрекеттері көбінесе белгісіздік жағдайында орындалады. Тиісінше, есептің тұжырымы және нәтижелері дәл болуы мүмкін емес. Егер нақты тәсілмен объективті функцияның экстремалды мәні оның сарапануына қатысты кейбір шарттарды орындау кезінде бар болса және оны табуға болатын болса, онда нақты емес тәсілмен жеткіліксіз хабардарлық шешімнің қабылданбауына әкелуі мүмкін, ал ақпараттандыру объектісін қорғаудың мақсаты берілген шектеулермен жеткілікті түрде қамтамасыз етілмеуі мүмкін. Қазақстанның цифрлық трансформациясының үдей түсуімен, соған сәйкес киберқауіптердің күрделене беруімен және халықаралық деңгейдегі жаңа әдістемелерді еліміздің тәжірибесіне бейімдеудің қажеттілігімен айқындалады.

1 КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН АДАПТИВТІ БАСҚАРУ БОЙЫНША ЗЕРТТЕУ ЖӘНЕ ТАЛДАУ

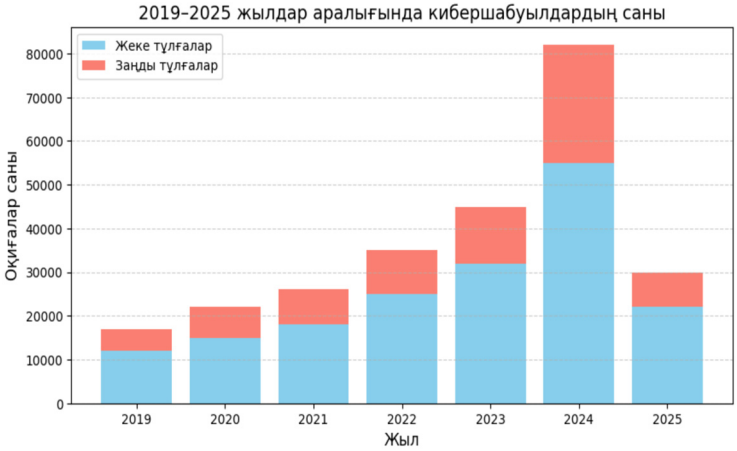
1.1. Қорғау тарабының ресурстарын бөлу есептері үшін ақпараттық қауіпсіздік модельдерін талдау

Шектеулі ресурстарды тиісінше бөлу көптеген экономикасы дамып келе жатқан мемлекеттердің болмысын және сонымен бірге операцияларды зерттеу бағыттарының бірі – ұйымдық жүйелерді ұтымды басқару әдістерін әзірлеумен айналысатын ғылым саласын құрайды [1]. Ақпараттық және кибернетикалық қауіпсіздікке қатысты мұндай тәсіл қорғау объектілері арасында ресурстарды бөлуді ұтымды шешу есебін қоюға әкеледі. Мұндай объектілерге компьютерлік жүйелердің архитектурасына қарай (жергілікті, бөлінген) мыналар жатқызылуы мүмкін: үй-жайлар; ақпарат тасымалдағыштар; байланыс желілері және т.б. Бұл тапсырманың бірнеше аспектілері бар және шешім әдістемесін таңдауды және түпкілікті нәтижені анықтайтын жағдай туралы белгілі бір білімді қажет етеді. Қорғау объектілерінің әрқайсысы туралы мұндай білімге мыналар жатады: ақпараттық ресурстардың саны, сапасы және маңыздылығы; ақпараттық ресурс қорғалуының бар деңгейі; оқиғаның күтілетін ықтималдығын ескере отырып, шабуыл жасау тарабы (немесе тараптар) бағыттай алатын ресурстардың (материалдық, қаржылық, адами, т.б.) саны; ақпараттық ресурстардың жеткілікті болуы үшін қажетті ресурстардың саны; ақпараттандыру объектісін қорғау тарабы бөлуі мүмкін ресурстар саны; ақпараттық ресурс жоғалту тәуекелінің жол берілетін деңгейі [2, 3]. Қорғаныс және шабуыл тараптарының тұрақты қарсылығы жағдайында ақпаратты қорғау қызметінің мақсаты шабуылдаушы тараптың әрекеттерінің салдары ретінде оны ұрлау, бұрмалау, құпиялылықты жоғалту мүмкіндіктерін азайту болып табылады. Сонымен қатар, шабуылдаушылар диаметрлі қарсы есептерге ие: өзінің ресурстарын ақпараттық ресурс ақпараттандыру объектісіне қол жеткізу шығындарын азайту үшін тарату. Ақпараттық саладағы қарсыласу көрсеткіштерінің статистикасы

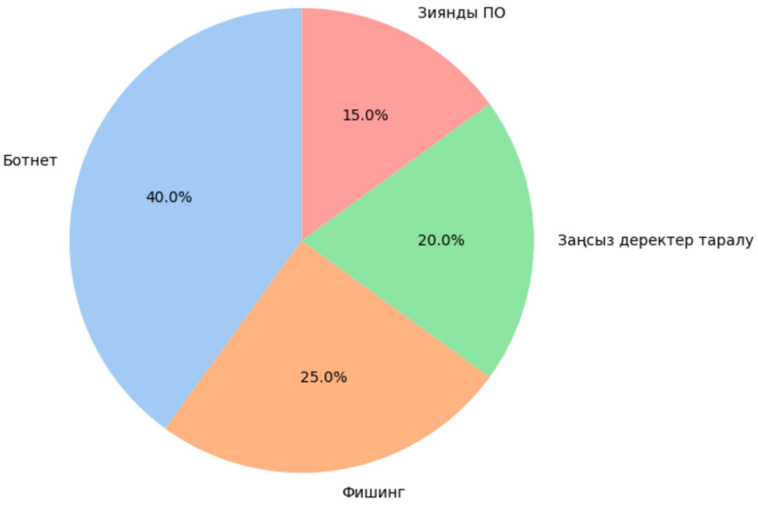
[4-6], 1.1-1.4 суретті қараңыз, ақпарат ағынының үнемі өсуіне және олардың маңыздылығына байланысты кибершабуылдардың қарқындылығы артып келе жатқанын көрсетеді. Сурет 1.1 деректеріне сүйенсек, 2019 жылдан 2025 жылға дейін жеке және заңды тұлғаларға жасалған кибершабуылдардың саны тұрақты өсіп келеді: 2019 жылы жалпы 17 000 оқиға тіркелсе, 2024 жылы бұл көрсеткіш 82 000-ға жеткен. 2025 жылдың алғашқы бес айында ғана 30 000 оқиға тіркелген, бұл жыл соңына қарай көрсеткіштің 100 000-ға жету ықтималдығын көрсетеді.Шабуыл түрлерінің үлестік көрсеткіштерін Сурет 1.2 бейнелейді: 2025 жылдың алғашқы бес айында ең көп таралған шабуылдар – ботнет (40%), фишинг (25%), заңсыз деректердің таралуы (20%) және зиянды бағдарламалар (15%). Бұл деректер қорғаныс стратегияларын жоспарлауда шабуылдардың нақты бағытын анықтауға мүмкіндік береді. Кибершабуылдардың өсу динамикасын Сурет 1.3 көрсетеді. Сызықтық графиктен көрініп тұрғандай, шабуылдардың жалпы саны (жеке және заңды тұлғаларға жасалған) жыл сайын артып келеді, бұл ақпараттық қауіпсіздік жүйелері тарапынан алдын ала шараларды қабылдаудың қажеттілігін көрсетеді.

Сонымен қатар, секторлық бөліністі Сурет 1.4 бейнелейді: қаржы саласы ең көп шабуылға ұшыраған (12 000 оқиға), денсаулық сақтау (5 000), мемлекеттік органдар (7 000), білім беру (3 000) және басқа секторлар (3 000). Бұл көрсеткіштер әр секторға арналған қорғау ресурстарын дұрыс бөлу қажеттігін айқындайды.Алайда, шабуылдардың бағыты уақыт өте келе өзгеруі мүмкін, өйткені шабуылдаушылардың объектілер арасындағы ақпаратқа қол жеткізу стратегиясы әрдайым жаңарып отырады. Мысалы, барлау кезеңі шабуылдаушылар үшін тиімді болса, олар өз ресурстарын мақсатқа тиімді бағыттауы мүмкін. Мұндай жағдайда қорғаныс тарапы өз ресурстарын шабуылдаушылардың тактикасына сәйкес қайта бөлуге мәжбүр болады (Сурет 1.2 және 1.4). Ресурстарды әзірлеу, енгізу, қызмет етуі, мониторингілеу, талдау, қолдау, жетілдіру және қарқынды басқару контексінде қорғау тараптары ақпараттық-коммуникациялық жүйе үшін ақпараттық қауіпсіздік тәуекелдерін ескеретін жалпы басқару жүйесінің бөлігі ретінде ақпараттық қауіпсіздік (киберқауіпсіздік) басқару жүйесі өзекті болып табылады. Ақпараттық қауіпсіздік басқарудың стандарттанған модельдері белгілі [9, 10]. Шешілетін есептің мәтінінде

«жоспарла - орында - тексер - әрекет ет» моделі кеңістігіндегі ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздік басқару әдістемесін әзірлеудің келешегі зор болып табылатынын ескертеміз [11].Ақпараттандыру объектісі ақпараттық қауіпсіздік басқару тұжырымдамалары: ақпараттық қауіпсіздік қағидаттары, активтер, қауіптер, әлсіздіктер, әсер ету, тәуекел, қорғау шаралары мен шектеулер негізінде қалыптастырылды [12]. Ақпаратты қорғаудың кешенді жүйелерінің тиімді жұмыс істеуі үшін ақпараттық қауіпсіздіктің мынадай жоғары деңгейлі қағидаттары іргелі болып табылады: Тәуекел менеджменті – активтер тиісті шаралар қабылдау арқылы қорғалуы керек. Қорғау шараларын таңдау және қолдану тәуекелдерді басқарудың тиісті әдіснамасы негізінде жүзеге асырылады. Әдістеме ақпараттандыру объектісі активтеріне, қауіптерге, әлсіздіктерге және қауіп-қатердің әртүрлі сипатына байланысты таңдалады. Әдістеме рұқсат етілген тәуекелдерді белгілейді және бар шектеулерді ескереді; Есептемелер – ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздік саласында және тәуекелдерді басқаруда маңызды рөл атқарады. Есептемелерді қалыптастыру үшін ақпараттық қауіпсіздіктің (АҚП) нақты саясаттарын іске асырудың әлсіз және күшті жақтарын анықтау қажет; Қызметтік есептер және жауапкершілік. Ақпараттандыру объектісі басшысы мен менеджменті ақпараттық қауіпсіздік активтерін (ақпараттық ресурстар) қамтамасыз етуге жауапты; қызметтік есептер мен жауапкершілік ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздікпен байланысты және айқындалуы, персоналдың назарына жеткізілуі тиіс [12, 125-126 б.]; Ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздікпен байланысты тәуекелдерді басқару процесінде мақсаттарды, стратегияларды және АҚП-ны назарға алған жөн; Өмірлік циклды басқару – ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздікте басқару тұрақты болуы керек (ақпараттық-коммуникациялық жүйе өмірлік циклі бойында).

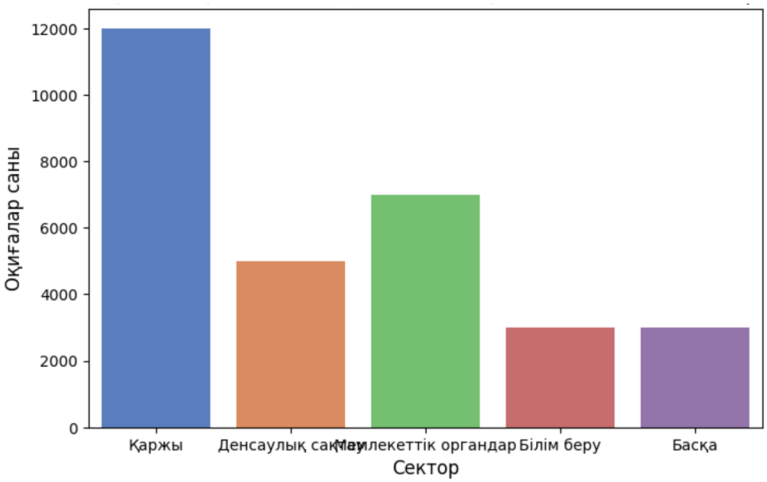


1.1-сурет. Жыл сайын тіркелген кибероқиғалар (2019–2025)



1.2-сурет. 2025 жылдың алғашқы бес айындағы шабуыл түрлері (пайыз)

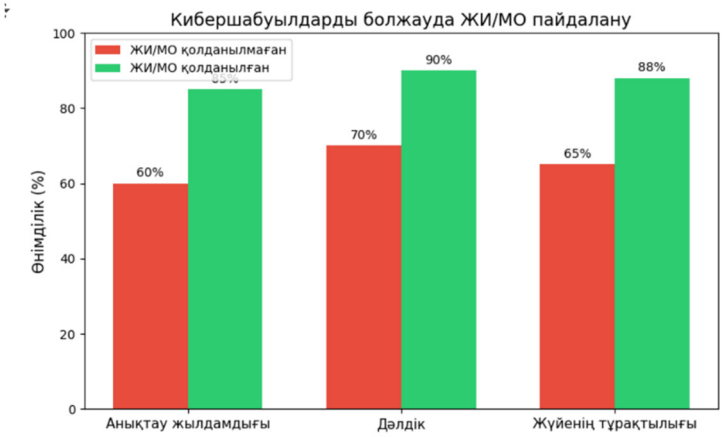
1.3-сурет. Кибершабуылдардың өсу динамикасы (2019–2025)



1.4-сурет. 2025 жылдың алғашқы бес айындағы салалық бөлініс бойынша кибершабуылдар

Заманауи әдістер: Жасанды интелект және ифрлық егіздер. Жасанды интеллект (ЖИ) пен машиналық оқыту (МО) киберқауіпсіздікті жаңа деңгейге көтеріп, барған сайын күрделене түсетін қауіптерді тану және оларға әрекет ету қабілетін айтарлықтай жақсартып жатыр. Бұл технологиялар үлкен көлемдегі деректерді жылдам әрі дәл талдап, әсіресе қауіптерді нақты уақыт режимінде анықтауда төңкеріс жасады. Мысалы, ЖИ әдеттен тыс желілік

трафик үлгілері немесе пайдаланушы әрекеттеріндегі күтпеген өзгерістер сияқты ықтимал бұзу немесе қауіпсіздік бұзушылықтарын көрсетуі мүмкін аномалияларды анықтай алады. Мұндай ерте ескерту сигналдары ұйымдарға қауіптерді азайту үшін шұғыл шаралар қабылдауға мүмкіндік береді [11]. Бұған қоса, қайталанатын бақылау тапсырмаларын автоматтандыру арқылы AI және ML операциялық тиімділікті жақсартады, бұл талдаушыларға стратегиялық шешімдер қабылдауға назар аударуға мүмкіндік береді. Мысалы, [12] 1.5-суретте маңызды киберқауіпсіздік негізгі өнімділік көрсеткіштері берілген және осы технологияларды пайдалану анықтау жылдамдығын, дәлдігін және жүйенің тұрақтылығын қалай жақсартқанын көрсетеді. Киберқауіпсіздік жүйелерінің тұрақтылығын арттырумен қатар, мұндай интеграция компанияларға өзгеретін кедергілерді жақсы жеңуге мүмкіндік береді.



1.5-сурет. Кибершабуылдарды болжауда ЖИ/МО пайдалану

Ұлттық қауіпсіздік үшін нақты уақыттағы қауіптерді анықтау мен болжауды жақсартатын ЖИ негізіндегі шешімдер ЖИ және МО үлгілерінің тіркесімін қамтиды. Оған қоса, машиналық оқыту үлгілері ақпараттық технологиялар, денсаулық сақтау, көлік, су мен санитария сияқты әртүрлі салаларда жақсы жұмыс істейтіні көрсетілген. Ақпаратты қорғау объектілері үшін үлкен тілдік модельдер (LLM) қолданбаларының тиімділігін арттыру мақсатында олардың өмірлік циклін қауіпсіздік пен орнықтылықтың үштік

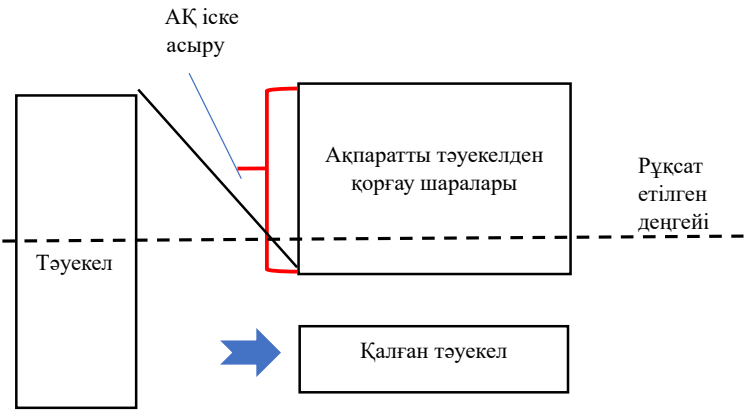
моделіне сәйкестендіру маңызды. Бұл мақсатқа жету үшін келесі нұсқаулықты қолдануға болады. Көзқарас және ауқымы: Ақпаратты қорғау объектілері жобасының бағытын анықтау. Жобаның негізгі мақсатын айқындау қажет. Мысалы, модель қауіптер туралы ақпаратты талдай ма, осалдықтарды бағалауға көмектесе ме немесе төтенше жағдайларға әрекет етуді қолдай ма? Сондай-ақ, қорғау шаралары қандай инфрақұрылым салаларына бағытталатынын анықтау керек.Модельді таңдау: Ақпаратты қорғау объектілері талаптарына сәйкес модель таңдалуы тиіс. Бұл ретте қауіпсіздік пен сенімділікке, яғни деректердің құпиялылығын қамтамасыз ететін модельді таңдау немесе әзірлеу маңызды. Сонымен қатар, қолданыстағы үлкен тілдік модельді (LLM) ақпаратты қорғау объектілеріне қатысты деректермен байытып бейімдеу немесе жаңа модельді әзірлеу жолдары қарастырылуы мүмкін.Тиімділік және үлгіні бейімдеу: CIP тиімді болуын қамтамасыз ету үшін модельдің өнімділігін бағалау қажет. Ол инфрақұрылымға төнетін қауіптерді анықтау, жіктеу және болжау қабілетін көрсетуі тиіс. Бұған қоса, модель сындарлы инфрақұрылымға төнетін нақты қауіптерге бейімделуі керек.Бағалау және қайталау: CIP дәлдігін жетілдіру үшін арнайы метрикалар қолданылады. Мысалы, модельдің қауіптерді анықтау дәлдігі, жауап беру жылдамдығы және салаға тән деректерді өңдеу қабілеті сияқты көрсеткіштер сындарлы инфрақұрылымды қорғау контекстінде бағалануы қажет.LLM-ді ендіру: Соңғы кезеңде модельді CIP (сындарлы инфрақұрылымды қорғау) үшін іске қосу жүзеге асырылады. Барлық аталған қадамдар 1.6-суретте көрсетілгендей бейнеленуі мүмкін. Генеративті жасанды интеллект пен үлкен тілдік модельдер (LLM) сындарлы инфрақұрылымды қорғауды сөзсіз жақсарта алады [13].

1.6-сурет. LLM дәрежесіне өтінімді толтыру қадамдары

1.7-сурет. Цифрлық егіздердің түрлері

Біздің зерттеуімізде цифрлық егіздер қолданбалары ықтимал кибершабуылдар мен тиісті қорғаныс шараларының контексінде жіктелді. Бұл зерттеу әртүрлі салалардың негізгі қауіп-қатерлерін анықтап, оларға қарсы тиімді стратегияларды ұсынады. Энергетика секторы, ұлттық инфрақұрылымның негізі ретінде, желіні басқару манипуляциясы, энергия ұрлығы және жабдықтау тізбегіне шабуылдар сияқты қауіптерге осал болып табылады. Бұл қауіптер энергиямен жабдықтаудың бұзылуына әкеліп, экономи-калық тұрақтылық пен қоғамдық қауіпсіздікке қатер төндіруі мүмкін. Осы қауіптерге қарсы күресу үшін нақты уақыт режиміндегі мониторинг жүйелері, шабуылдарды анықтау жүйелері (IDS) және қауіпсіз байланыс протоколдары қолданылады. Бұл технологиялар аномалияларды анықтауға, қауіптерді жедел азайтуға және энергетикалық жүйелердің тұтастығын сақтауға көмектеседі. Денсаулық сақтау секторы кибершабуылдарға, соның ішінде пациенттердің деректерінің бұзылуы, бопсалаушы бағдарламалар шабуылдары (ransomware) және қызмет көрсетуден бас тарту (DoS) шабуылдарына ерекше осал. Бұл қауіптер денсаулық сақтау ақпаратының құпиялығына және маңызды медициналық қызметтердің жұмыс істеуіне қатер төндіреді. Негізгі қорғаныс шараларына

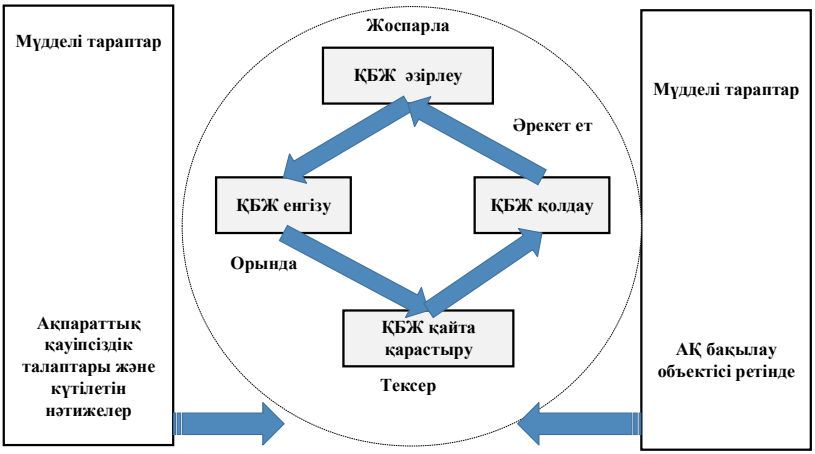
HIPAA талаптарына сәйкестік, соңғы нүктелерді қорғау (endpoint protection) және апаттан кейін қалпына келтіру жоспарлары кіреді. Бұл шаралар денсаулық сақтау деректерінің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған [14]. Білім беру секторы да академиялық деректердің бұзылуы, жеке бас мәліметтерінің ұрлануы және алаяқтық сияқты киберқауіптерге тап болады. Бұл қауіптер білім беру мекемелеріне деген сенімді төмендетіп, студенттер мен қызметкерлердің жеке мәліметтерінің қауіпсіздігін бұзуы мүмкін. Негізгі қорғаныс шаралары сенімді деректерді қорғау саясатын әзірлеу, пайдаланушыларды киберқауіпсіздікке үйрету және қауіпсіз тестілеу мен бағалау орталарын құруды қамтиды [15]. Бұл мәселелер бейімделгіш, салаға бағытталған киберқауіпсіздік стратегияларын әзірлеудің қажеттілігін көрсетеді. Озық технологияларды пайдалану, реттеуші стандарттарды сақтау және киберқауіпсіздік туралы хабардарлық мәдениетін қалыптастыру сындарлы инфрақұрылымның орнықтылығын арттырып, оның тұрақтылығы мен қауіпсіздігін қамтамасыз ете алады [16]. Ақпараттық қауіпсіздік саясаты ақпараттық қауіпсіздік қағидаттарынан және тұтастай алғанда ұйымның (компанияның, кәсіпорынның) директиваларынан тұруы мүмкін. Кейбір жағдайларда ол техникалық немесе басқару саясатына қосылуы мүмкін. Бұл саясаттар жиынтығында ақпараттық қауіпсіздік саясатының негізін құрайды.



1.8-сурет. Ақпаратты қорғау шаралары мен тәуекелдердің өзара байланысының моделі

Басқару түрлерінің, АҚО өлшемдері мен құрылымдарының айырмашылығы процестің қоршаған ортаға бағдарын тудырады.

«Жоспарла – орында – тексер – әрекет ет» моделі (1.9-сур.) бұдан әрі барлық ақпараттық қауіпсіздікті басқару жүйесіне қолданылады (кейбір авторларда ақпараттық қауіпсіздікті қамтамасыз ету жүйесі немесе [12, б.76]). Ол ақпараттық қауіпсіздікті қамтамасыз ету жүйесі регламенттелген процестердің көмегімен мүдделі тараптардың талаптары мен болжалдарына – кіріс деректеріне сәйкес келетін ақпараттық қауіпсіздік шығыс деректерін қалай жүргізетінін суреттейді.



1.9-сурет. «Жоспарла - орында – тексер - әрекет ет" ақпараттық қауіпсіздік моделі

«Жоспарла – орында – тексер – әрекет ет» моделіне сәйкес АҚО ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздікті басқару кезеңдерінің мазмұны 1.1-кестеде келтірілген. Қорғаныс ресурстарын адаптивті басқару және шабуылдаушы тарапқа белсенді қарсы тұру, сондай-ақ ақпараттық қауіпсіздік және киберқауіпсіздік тәуекелдерін басқару процесін құру кезінде ISO/IEC 17799, ISO/IEC 27001 және CobiT (Control Objectives for Information and related technology), сонымен қатар NIST (National Institute of Standards and Technology) халықаралық стандарттарының ережелері мен талаптарын ескеретін әдістер қолданылады [13, 14].Сондай-

ақ бірқатар авторлардың зерттеулері мен тәжірибелері [15-17] негізінде әзірленген бірегей әдістемелер, сондай-ақ әлемдік практика мен халықаралық стандарттар, жүйелік талдау мен жобалаудың құрылымдық әдістеріне негізделген арнайы аспаптық құралдар (SSADM-Structured Systems Analysis and Design) пайдаланылады. Бүгінгі таңда ақпараттық-коммуникациялық жүйе және олардың ақпаратты қорғау құралдарына қойылатын ең маңызды тұжырымдамалық талап - икемделу талабы [18]. Мұндай қызметке ақпаратты қорғау құралдары нақты ұйымдастыруға және тұрақты басқаруға негізделуі керек. Ақпараттық-коммуникациялық жүйедегі басқару деп оның жұмыс істеуінің әр кезеңінде жүйенің элементтеріне мұндай бақылау әсерін анықтау деп түсініледі, нәтижесінде бір немесе бірнеше функционалды есептерді шешуге болады. Функционалдық есептер деп АТЖ іске асыратын функционалдық қатынастағы біртекті операциялар жиынтығын айтады [18, 129-б.]. Қазіргі заманғы компьютерлік техниканың даму деңгейі ақпараттық қауіпсіздікті басқарудың тиімділігін арттыру және автоматтандыру үшін ақпараттық-коммуникациялық жүйе қауіпсіздігін басқару орталығында қолданылатын шешім қабылдауды қолдаудың ішкі жүйелерін ақпаратты қорғау құралдары құрамына қосуға мүмкіндік берді. Ақпаратты қорғау құралдары декомпозициясының нәтижесінде үш ұйымдастыру бөлігін бөлуге болады: ақпараттық қауіпсіздікті қамтамасыз ету тетіктері; ақпараттық қауіпсіздік механизмдерін басқару механизмдері; Жүйе жұмысын жалпы ұйымдастыру тетіктері.

«Жоспарла – орында – тексер – әрекет ет» моделіне сәйкес ақпараттандыру объектісі ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздікті басқару кезеңдерінің мазмұны келесідей болады:

1-кезең. Ақпараттық қауіпсіздікті басқару жүйесі жоспарлау (әзірлеу). Жалпы ақпараттық қауіпсіздік саясаттары мен мақсаттарына сәйкес келетін нәтижелерге қол жеткізу үшін тәуекелдерді басқару және ақпараттық жүйе жақсарту үшін маңызды ақпараттық қауіпсіздікті басқару жүйесі саясатын, мақсаттарын, процестерін және процедураларын әзірлеу.

2-кезең. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесі орындау (енгізу және жұмыс істеуін қамтамасыз ету). Ақпаратты қорғау құралдырының жұмыс істеуін енгізу және қамтамасыз ету,

ақпараттық қауіпсіздікті басқару жүйесі процестері мен рәсімдерін бақылауды жүзеге асыру.

3-кезең. Ақпараттық қауіпсіздікті басқару жүйесін тексеру (мониторингті және қайта қарауды (түзетуді) жүзеге асыру). Ақпараттық-коммуникациялық жүйе процестерінің өнімділігін ақпараттық қауіпсіздікті басқару жүйесі саясатына, мақсаттарына және практикалық тәжірибесіне сәйкес бағалау және мүмкіндігінше өлшеу. Қажет болған жағдайда ақпараттық қауіпсіздікті басқару жүйесіне түзетулер енгізу үшін басшылыққа нәтижелер туралы есеп беру.

4-кезең Әрекет (ақпараттық қауіпсіздікті басқару жүйесін қолдау және жетілдіру). Ақпараттық қауіпсіздікті басқару жүйесін тұрақты жетілдіруге қол жеткізу үшін, оның ішінде қорғау ресурстарын адаптивті түрде қайта бөлу қажет болған жағдайлар үшін ақпараттандыру объектісінің басшысы, ақпараттық қауіпсіздік қызметтері немесе басқа да маңызды ақпарат тарапынан ақпараттық қауіпсіздікті басқару жүйесін ішкі аудит және қайта қарау нәтижелері негізінде түзету және алдын алу іс-шараларын пайдалану.

Қарсы қорғаныс шараларының бірі – ресурстарды бейімделме басқару. Бұл ретте ресурстарды бөлу қорғаныс тарабы үшін нақты шабуылдың мақсатын анықтау қажеттілігінен туындаған кідіріспен жүргізіледі [19]. Осылайша, қорғаныс ресурстарын адаптивті басқару есептерінде шешімдерді қолдау үшін әдістерді, модельдерді және сәйкес алгоритмдерді әзірлеу есебі туындайды. Мұнда әзірленген шешімдер үнемі өзгеріп отыратын жағдайларда қорғаныс жағы үшін ұтымды көрсеткіштерге қол жеткізуді қамтамасыз етуі керек. Ойын теориясының терминологиясын қолдансақ, онда позициялық ойынмен істес боламыз. Сол кезде жоғарыда айтылғандарға сәйкес бірқатар сұрақтар туындайды. Осы ойында мақсатты функциямен анықталған мән үшін ершік нүктесі қандай жағдайда болады және оның жағдайына қарсы тұру шарттары қалай әсер етеді: шабуыл (H) және қорғаныс (D) ресурстарының салыстырмалы саны (Z=H/D), объектілер (k – объект нөмірі), объектілердің әлсіздігі {Vk} арасында ақпараттық ресурс бөлу {gk}. Ершік нүктесі болмағандағы белгісіздік жағдайында қорғау ресурстарын бөлу {dk} қандай болуы тиіс. Шабуылдардың бағыттылығы белгілі болған жағдайда, жалпы шығындар ең аз болатындай етіп, әртүрлі әлсіздігі бар объектілер

арасында ақпараттық ресурстарды {gk} қайта бөлу қалай болады. Келесі шамаларды айқындайтын ұтымдылықтың әртүрлі критерийлерін және әртүрлі мақсат функцияларды пайдалану кезінде басқару алгоритмдері қалай ерекшеленеді: жоғалған ақпараттық ресурс саны; ақпараттық ресурс инвестицияларынан түсетін пайда; ақпараттық ресурс рентабельділігі; және көп мақсатты функцияны пайдалану кезінде нәтиже қандай болады. Тараптардың әрқайсысы өз ақпаратын қорғауға арналған ресурстардың бір бөлігін, ал екіншісін қарсыластың іс-әрекеттері туралы ақпарат алуға жоғалтқан кезде кешенді қарсыласуда басқару алгоритмі қандай болады. Ақпараттық қауіпсіздік және киберқауіпсіздік менеджментінің математикалық модельдерінде көрсетілгендей [20-22], мақсатты функция, әдетте, белгілі бір дәрежеде ақпараттық қауіпсіздік жүйесінің әлсіздігі арқылы қарсыласу көрсеткіштерінің бірін (көбінесе оның ұтымды мәнін) айқындайды. Мысалы, Гордон-Лоеб моделінде бұл көрсеткіш ақпаратты қорғау құралдарына инвестиция салу арқылы ақпараттық ресурс жоғалуынан болатын шығындардың азаюы болып табылады. Өз кезегінде, Қорғаныс объектісінің әлсіздігі, егер қорғаныс шығындары нөлге тең болса, шабуылдың сәтті болу ықтималдығы ретінде қарастырылады.

Соңғы онжылдықта ақпараттық қауіпсіздік есебін сипаттайтын кем дегенде ондаған модель пайда болғанын ескертеміз. Ең көп тарағаны – Гордон-Лоеб моделі. Бұл модельдің мақсаты ақпаратты қорғауға инвестициялардың ұтымды мөлшерін анықтау есебін шешу болып табылады. Модельдің басты ерекшелігі - ақпараттық қауіпсіздік деңгейін анықтайтын әлсіздік функциясын енгізу және дамыту.

Төменде ұқсас модельдер мен олардың нұсқаларының өте көп екенін ескере отырып, ақпараттандыру объектісі ақпараттық қауіпсіздікті басқаруды ұтымды шешу саласындағы барлық қызықты және сұранысқа ие модельдер жүйеленген, сонымен қатар олардың күшті және әлсіз жақтары келтірілген.

Гордон-Лоеб моделі. Бұл модельдегі басты нәрсе – ақпараттық қауіпсіздік деңгейін анықтайтын әлсіздік функциясын енгізу және әзірлеу. Негізгі параметрлер: ақпараттың жайылып кетуінен болатын ықтимал шығындар; шабуыл жасау ықтималдығы; ақпараттық ресурс әлсіздігі; ақпараттық қауіпсіздікке арналған шығындар; шабуыл нәтижесінде болатын шығындар ықтимал-

дығы; ақпараттық қауіпсіздікке инвестициялар болмаған кездегі ықтимал шығындар; ақпараттық қауіпсіздік және киберқауіпсіздік бұзу ықтималдығы сияқты параметрлерген тоқталған. Модельдің артықшылығы деп алғаш рет қорғаныс пен шабуыл арасындағы қарама-қайшылықты қарастыруда маңызды болып табылатын әлсіздік функциясы анықталғанын айтуға болады. [23]

Гросс моделі. Модельге сәйкес, қақтығысушы тараптардың ресурстары *(D), (H)* бар және олардың қарсыласу нәтижесі мақсатты функциямен анықталады, ол салынған ресурстардың айырмашылығына сызықты тәуелді болады және сызықты бағдарламалау есебіне әкеледі. Негізгі параметрлер *k*- объектідегі шабуыл және қорғаныс ресурстары, объектілердің маңыздылығын немесе олардың әлсіздігін білдіретін салмақ коэффициенті деп білеміз. Бұл модельдің қарапайымдылығы басты артықшылығы болады. .[24]

Задирак В.К. моделі. Модельде мақсатты функция ақпараттың жайылып кетуінен болатын шығындар мен оны қорғау шығындарының мөлшерін анықтайды. Жағдайды сипаттайтын теңдеулер жүйесін шешу ақпаратты қорғауға арналған мақсатты шығындарды ұтымды шешуге сәйкес келетін шамалар үшін мәндер кестесін алуға мүмкіндік береді. Бірақ шабуыл тарапының ресурстары ескерілмейді және адаптивті режимдегі ұтымды шешім есебі жоқ [25].

Фомченкова Л.В. моделі. Модель ұйымның ақпараттық қауіпсіздігімен байланысты ішкі қауіптер мен тәуекелдердің біріктірілген идентификаторы негізінде, сондай-ақ сандық әлеуетті, бизнесті және ақпараттық технологиялар стратегияларын ескере отырып, ақпараттық қауіпсіздікті басқару саласындағы шешімдерді қалыптастыруға, қажетті ақпараттық қорғаудың дәрежесі мен әдісін анықтауға мүмкіндік береді. Сонымен қатар ұйымдағы ақпараттық қауэпсіздікті бақылау функцияларына бағытталған [26] .

Калашников А. О. моделі.

Модель сыни инфрақұрылымның ақпараттық қауіпсіздікті басқарудың кейбір аспектілерін оның ауытқыған күйлерін анықтау негізінде сипаттайды. Кешенді бағалау, жүйелік және кластерлік талдау алгоритмдері қолданылады. Кластерлік талдау алгоритмдерінің арқасында объектілерді қарастырылатын объектілердің түріне ешқандай шектеулер қоймай, бірқатар белгілерге сәйкес бөлуге болады Модель жүйеде ауытқулар туралы статистика болған жағдайға ғана бағытталған [28].

Котенко И.В. моделі. Ақпараттық қауіпсіздікті басқарудың зияткерлік тетіктерін іске асыруға негізделген. Киберқауіпсіздікті басқару ақылды агенттер, шабуылдаушының жалған ақпарат беру механизмдері, жасыру және камуфляжға негізделген. Жоғары есептеу күрделілігі. Адаптивті режимде модельді және есептеу нәтижелерін қолдануға арна лған параметрлер жоқ. Бірақ модельдің кешенділігін артықшылығы ретінде бағаланайды [29, 30].

Глушак, В. В., Новиков және Архипов модельдері. Модель тәуекелдің ықтималды параметрлерін анықтауға арналған. Жағдайды сипаттау үшін: шабуылдаушының қауіп-қатерді жүзеге асыру шығындары; шабуылдаушының алған «ұтысы», қорғаныс тарапынан келтірілген залалды қарастырғанмен, қорғаныс объектілері арасында ресурстарды бөлуді ұтымды шешу есебі қарастырылмады [31-34].

Ахметов-Лахно-Малюков модельдері ойын теориясының негіздеріне құрылған және қорғаныс пен шабуыл ресурстары арасындағы қарама-қайшылық контекстінде жағдайды қарастырады. Модельдер қорғаныс тарапының қаржылық стратегияларын таңдауды ұтымды шешу қажет болған барлық жағдайларды қамтиды. Дегенмен, модельдердің есептеу күрделілігі жоғары. шешім қабылдауды қолдау жүйесі қолданбай есептеу өте қиын [35].

Ресурстарды басқаруды математикалық модельдеу саласындағы ғылыми жұмыстарды талдау ақпаратты қорғау тараптары негізгі күш-жігердің қорғауға салынған инвестициялар көлемін анықтауға бағытталғанын көрсетті (1.1-кесте.). Бұл инвестицияларды қорғау объектілері арасында бөлу есептеріне жеке зерттеулер ғана арналған. Сонымен қатар, қолданыстағы әзірлемелер шабуылдаушының ықтимал әрекеттері мен олардың салдарының ақпаратты тандыру объектісіндегі ақпараттық жүйе көрсеткіштері мен сипаттамаларының өзгеруіне әсерін сирек ескереді.

Жоғарыда келтірілген ғылыми жұмыстарды талдау нәтижесінде шаруашылық қызмет субъектілерінің ақпаратын қорғауға бөлінетін шектеулі қаржы ресурстарын тиімді пайдалану есебі барған сайын маңызды бола түсуде және айтарлықтай дәрежеде кез келген мемлекеттің ақпараттық қауіпсіздік және киберқауіпсіздік деңгейін айқындайды [36]. Сонымен қатар, белгісіздік жағдайында, шабуылдаушы тараптың әрекеттерінің дәйектілігі алдын-ала белгісіз және белгілі бір ықтималдықпен ғана мақсатты шабуыл сценарийін болжауға болатын кезде, теориялық-ойын әдістерін қолдану және

қарама-қайшылық жағдайларының өзгеру адаптивтілігін ескере отырып, ақпараттық қауіпсіздік объектілері арасында шектеулі ресурстарды ұтымды бөлуді іздеу қаржылық шығындарды ақпараттық ресурстардың жайылып кетуінен азайтуға мүмкіндік береді.

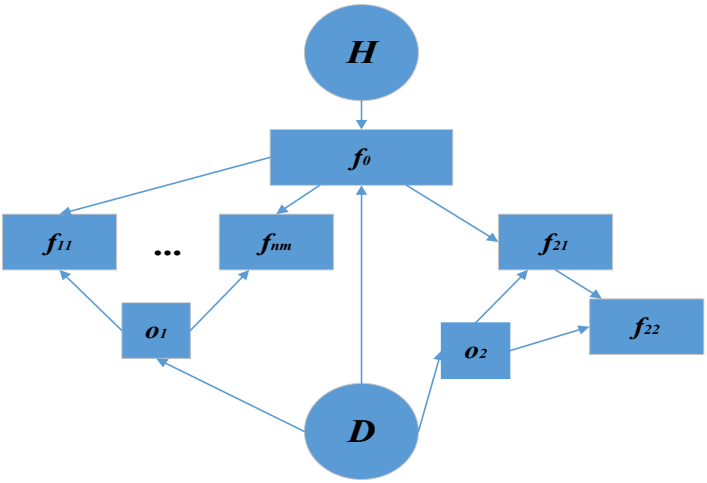
Ақпараттық қауіпсіздік және ақпараттандыру объектісі киберқауіпсіздік саласындағы көптеген зерттеулер көрсеткендей, ақпараттың көлемі мен құнының өсуі ақпаратты қорғау құралдары тиесілі қиындауына алып келеді. Қазіргі заманғы ақпаратты қорғау құралдары көп деңгейлі және көп контурлы болып келеді.

Ақпаратты қорғау құралдары құнының өсуі қорғау ресурстарын ұтымды пайдалану есебін өзекті етеді. Шешімдерді іздеу процесінде уақыт өте келе шабуылдаушы тараптың қарсыласу жағдайларының өзгеруін ескеру қажет. Бұл ақпараттық ресурстардың «қартаюына», олардың жаңаруына, жаңа шабуыл құралдарының пайда болуына, ақпаратты қорғау құралдары модернизациясына және т.б. байланысты. Нәтижесінде, біз күрделі қорғаныс құрылымдарындағы ресурстарды адаптивті басқару есебін шешу қажеттілігіне тірелеміз.

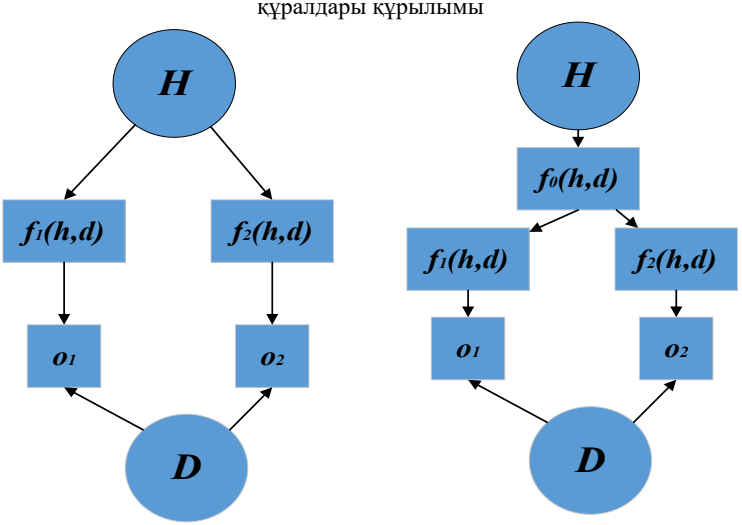
1.10-суретте мұндай құрылымның мысалы көрсетілген. Схема физикалық және электронды жүйелерді сипаттайды. Физикалық жүйенің мысалы f_0 шабуылдаушылар үшін жалпы кедергі аумақтың қорғалған периметрі болатын жүйе болуы мүмкін. Үй-жайдың o_1, o_2 – объектілері, ал f_{ij} – тиісті үй-жайларды қорғауға арналған құралдар. Мұнда i, j – индекстер, сәйкесінше, объектінің нөмірі, кедергі нөмірі болып табылады.

Бірінші объектінің f_{11}, f_{12}, f_{13} параллель қорғаныс құралдары, мысалы, электр және жылу желілерін жерге қосу, экрандау, үй-жайларды шулату. Екінші объектінің f_{21}, f_{22} бірізді қорғаныс құралдары іргелес бөлмелерде орналасқан. Электрондық жүйеде o_1, o_2 – объектілер – жалпы және жеке қорғаныс құралдары бар компьютерлер, серверлер. Мысалы, жалпы қорғаныс – бұл firewall. Тиісінше, жеке қорғаныс - бұл антивирустық бағдарламалық қамтамасыз ету. Күрделі схеманы декомпозиция әдістерімен қорғаныс элементтерінің параллельді

(1.11, а-сурет) немесе тізбекті-параллельді (1.11, б-сурет) орналастырып, қарапайым схемаларға (1.10-сурет) келтіруге болады.



1.10-сурет. Ақпараттандыру объектісі үшін ақпаратты қорғау құралдары құрылымы



а) б)

а – ақпараттандыру объектісі үшін бір деңгейлі ақпаратты қорғау құралдары;
б – ақпараттандыру объектісі үшін екі деңгейлі ақпаратты қорғау құралдары

1.11-сурет. Ақпараттандыру объектісі үшін жеңілдетілген ақпаратты қорғау құралдары схемалары

Көп тізбекті қорғаныс жүйелерінде ақпаратты қорғау ресурстарын бөлудің негізгі заңдылықтарын анықтау үшін жеңілдетілген құрылымдарды қарастырумен шектелуге болады (1.11-сурет.). Сонда, мысалы, кедергілердің бірізді-параллель орналасуын талдау (1.11-сурет, б) арқылы, келесі есептерді жеке немесе жиынтықта қарастыруға болады: (1.11-сурет, б) схема мен (1.11-сурет, а) схеманы салыстыру және ақпаратты қорғау тарапының бюджеті өзгермеген кезде қорғаудың қосымша элементін (кедергілер немесе бөгеуілдер) енгізудің орындылығын айқындау; қорғаудың жалпы элементтері (мысалы, файервол, қолжетімділікті бақылау жүйесі және т. б.) мен жеке қорғаныс құралдары (мысалы, вирусқа қарсы бағдарламалар, криптографиялық қорғау құралдары және т. б.) арасында ресурстардың ұтымды бөлінуін анықтау; қорғаныс ресурстарын бөлу схемаларының әртүрлі нұсқалары мен комбинациялары арасындағы корреляцияны зерттеу. Соңғысы ұтымды схеманы таңдау үшін орындалады; ақпараттандыру объектісі үшін көп контурлы ақпаратты қорғау құралдарында ресурстарды басқару бойынша ұсыныстар әзірлеу.

Ақпараттандыру объектісі ақпараттық инфрақұрылымын талдау кезінде, сондай-ақ ақпараттандыру объектісі ақпараттық жүйе тағайындалуын; ақпараттық жүйе мен оның ақпаратты қорғау құралдары функционалдық талаптарын; ақпараттық жүйе мен деректердің сыни болуын; ақпараттандыру объектісі желісінің ағымдағы топологиясын; жүйелік интерфейстерді; ақпараттық ағындарды; ақпараттандыру объектісі персоналын; енгізілген қауіпсіздік саясатын; ақпараттық жүйе үшін техникалық бақылау құралдарын және т. б. ескеру қажет. Осылайша, тиімді ақпаратты қорғау құралдары құру үшін кешенді түрдегі және оның тиімділігін анықтайтын көрсеткіштердің жеткілікті үлкен санын ескеру қажет. Сонымен қатар, олардың талаптарының сәйкес келмеуіне байланысты әртүрлі көрсеткіштердің ұтымды мәндеріне қол жеткізу өте қиын және көбінесе мүмкін емес. Нәтижесінде, біз көп критерийлі тапсырмаға тірелеміз. Мұндай есепті шешу әрқашан жеке көрсеткіштердің талаптарын қанағаттандыруда ымыраға келу болып табылады. Мұндай көп критерийліесептерді шешкен кезде әрқашан шешім алгоритмдерін таңдау дилеммасы болады. Егер мұндай әдістер мен алгоритмдерді жалпыласа, оларды екі тәсілге дейін азайтуға болады – анық және анық емес. Бұл жіктеуді

жеткілікті түрде шартты деп санауға болады. Бұл, әсіресе, ақпаратты қорғауға байланысты есептерге қатысты, өйткені қорғау тарапының әрекеттері көбінесе белгісіздік жағдайында болады. Тиісінше, есептің тұжырымы және нәтижелері дәл болуы мүмкін емес. Егер нақты көзқараспен объективті функцияның экстремалды мәні оның сарапануына қатысты кейбір шарттарды орындау кезінде бар және оны табуға болатын болса, онда түсініксіз жолмен жеткілікті түрде хабардар болмау шешімге қод жеткізуге мүмкіндік бермеуі ықтимал, ал ақпараттандыру объектісін қорғаудың мақсаты берілген шектеулермен жеткілікті түрде орындалмауы мүмкін.

1.2. Ақпараттандыру объектілерінің киберқауіпсіздік ресурстарын көп критерийлі ұтымды шешу мен адаптивті басқарудың математикалық әдістерін талдау

Кез келген процестерді немесе құбылыстарды жетілдіру әрқашан оларды сипаттайтын өлшемдерді анықтауға негізделген. Бұл өз кезегінде зерттелетін процестерді немесе құбылыстарды ұтымды шешуды қамтамасыз ету жолдарын қалыптастырудың жеткіліктілігінің алғышарты болып табылады. Сонымен қатар, көп контурлы жүйелерде ақпаратты қорғау құралдары ақпараттық ресурстарының тұтастығын, құпиялылығын және қол жетімділігін қорғау үшін жергілікті есептерге жауап беретін көптеген объектілері болады. Ақпараттандыру объектісі өмірлік циклі бойында аппараттық, бағдарламалық, ұйымдастырушылық құралдар мен қорғаныс әдістерінің әртүрлі конфигурацияларын қамтуы мүмкін мұндай көп контурлы жүйелерді зерттеу қиын есеп болып табылады. Әдетте, мұндай көп контурлы ақпаратты қорғау құралдарын жобалау немесе модернизациялау кезеңінде қорғаныс құралдарының құрамын көп критерийлі ұтымды шешуге байланысты есептерді шешу қажет. Бұл жағдайда қорғаныс ресурстарын адаптивті басқарудың аспектілерін ескеру керек. Мұндай көп критерийлі есептерді, ең алдымен, математикалық модельдеудің әртүрлі әдістерін қолдану және ақпараттандыру объектісі көп контурлы қорғаныс кешендерінің құрамын көп критерийліұтымды шешу арқылы шешу керек.

Бұл жағдайда мұндай көп критерийлі ұтымды шешу есептерін шешудің математикалық модельдері екі қарама-қайшылықты

талаптарға жауап беруі керек. Біріншіден, олар жүйенің қасиеттерін барынша көрсетуі тиіс. Екіншіден, түпкілікті нәтиже алуды қиындатуы мүмкін артық бөлшектенуден аулақ болуға тиіс. Сондай-ақ, келесі жағдайды ескеру қажет. Ақпараттандыру объектісі қорғаныс жағының адаптивті ресурстарын басқару есептері бұл тек ақпараттандыру объектісі киберқауіпсіздік контурындағы қорғаныс компоненттерінің санын көбейту арқылы шешілетін таза техникалық есеп емес. Бірақ бұл басқарушылық есеп те. Сонымен қатар, екінші есеп ақпараттық қауіпсіздік және киберқауіпсіздік менеджменті сияқты ұғыммен байланысты. ақпараттық қауіпсіздік және киберқауіпсіздік менеджментінің негізгі есебі ақпараттандыру объектісі үшін ақпаратты қорғау құралдары жұмыс істеу тиімділігінің техникалық ғана емес, экономикалық көрсеткіштерін де ұтымды шешу болып табылады. Осылайша, [37-40] жұмыстарда ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздік шығындарын ұтымды шешу есептері талданды. Негізінде көп критерийлітаңдау есебін шешу туралы сөз болады. Ақпараттандыру объектісі үшін ақпаратты қорғау құралдарына шығындарды бөлудің ұтымды нұсқасын таңдаудың интерактивті процедурасы ұсынылды. [41] жұмыста ақпараттандыру объектісі үшін ақпараттық қауіпсіздікті және киберқауіпсіздікті қамтамасыз ететін механизмдерді басқарудың әртүрлі функциялары арасында ресурстарды ұтымды бөлу есебінің алты түрлі тұжырымы келтірілген. Ақпараттық қауіпсіздікті қамтамасыз ететін жүйелерді жобалау сатысында да, Ақпараттық қауіпсіздік контурларын жетілдіру және дамыту кезеңдерінде де қолдануға арналған ресурстарды бөлу есебін қою ұсынылады. Авторлар ақпараттық қауіпсіздікті қамтамасыз етудің жеті негізгі функциясын анықтайды [42, 113-б.] және әртүрлі ақпаратты қорғау құралдары функциялары арасында қаражат бөлудің бөлшектеуге және рәсімдеуге арналған екі тәсілін ұсынады. Бірінші тәсіл ақпараттық қауіпсіздік қаражатының құрамы мен санын есепке алуға негізделген. Екінші тәсіл жалпыланған заңдылықтарды талдауға және ақпараттандыру объектісін ақпараттық қауіпсіздік құралдарымен қамтамасыз ету процесіне енгізілген қатынастар мен оларды қолданудың тиімділігіне негізделген. Жұмыста ықтимал және шығындар модельдері қарастырылған. Соңғысы зерттеушілер үшін үлкен қызығушылық тудырады, авторлар ұсынған бағдарла-

малық өнімге деректерді енгізу кезінде ресурстарды бөлу есебі параметрлерінің физикалық мағынасын нақтылайды.[43] жұмыста ақпаратты қорғау құралдары объектілері арасында ресурстарды бөлуді ойын моделі және объектілердің тең қауіпсіздігі қағидаты негізінде орындау ұсынылатын модель қарастырылады. Ресурстарды бөлу есебі екі ойыншы - қорғаушы және нөлдік шабуылшы турнирі ретінде тұжырымдалған. Әр ойыншы басқа ойыншының бекітілген шешімімен сызықтық бағдарламалау есептерін шешеді. Жұмыста кепілдендірілген нәтиже алу үшін дәйекті түрде қолдануға болатын үш алгоритм ұсынылған. Алгоритмдер математикалық негізделген, нәтижелер тест мысалдарымен расталған және жалпыланған. Ақпараттандыру объектісі ақпараттық қауіпсіздікті арттыруға бағытталған қаржы ресурстарын бөлудің ойын модельдері де жұмыста егжей-тегжейлі қарастырылған [44, 45]. Белгілі бір математикалық әдістерді жүзеге асыратын бағдарламалық қамтамасыз ету көпшілігі дайындалған кірістерге байланысты көптеген есептерді шешуге мүмкіндік беретін өте әмбебап өнімдер болып табылады. [46] жұмыста сипатталған бағдарламалық пакеттің басты ерекшелігі - есептеу операциялары мен жұмыс уақытының өлшемі бойынша ең тиімді алгоритмді таңдауға мүмкіндік беретін ақылды агенттің болуы. Сонымен қатар, ақпаратты қорғау құралдары құру кезінде ақпаратты қорғау құралдарының ұзақ мерзімді функционалдығын қамтамасыз ететін ресурстардың уақтылы бөлінуі де ескерілетіні өте маңызды. [46, 87-б.] жұмыста ақпаратты қорғау құралдарына бөлінетін ресурстарды бөлу есептерін шешу үшін бағдарламалық қамтамасыз ету сипатталған, 1.12-суретті қараңыз.

Шешім қабылдаушы тұлғаның жүйемен жұмысы «бұлтты» сервисте есепті шешу үшін құралдарды орналастыру талаптарын ескере отырып, online-режимде өтеді. Бұл пайдаланушыға қажетті бағдарламалық қамтамасыз етуді және оны орнатуды іздемей, есептің шешімін табуға мүмкіндік береді. Пакетке енгізілуі керек әдістерді таңдау кезінде зерттеу тапсырмасын орындау, тапсырманың түрін анықтау және сәйкесінше кіріс деректерін дайындау қажет болды. Ақпаратты қорғау құралдарында ресурстарды бөлуді модельдеу есебін шешу үшін бағдарламалық пакеттің прототипіне енгізілген бөлімдердің тізімі: ресурстарды бөлудің классикалық есептерін шешуге арналған бөлім (кәсіпорындар арасында ресурс-

тарды бөлу және қорларды басқару есептері); ресурстарды бөлудің желілік есептерін шешуге арналған бөлім (ең қысқа жолды табу және ең жоғары ағын туралы есептер);қолданбалы есептерді шешуге арналған бөлім (қатерлердің кейбір түрлерін жою есебінен ақпараттық қауіпсіздік тәуекелдерін төмендету мақсатында қаржы ресурстарын бөлу есебі енгізілген); әдістер мен алгоритмдерден тұратын бақылау бөлімі (шартты ұтымды шешу әдісі, бұтақтар мен шекаралар әдісі, алға және кері жүгіру алгоритмдері, Качмаж және Балаш алгоритмдері, генетикалық алгоритмдер және т.б.). Көп критерийлі ұтымды шешу есептерін қалыптастыру және оларды шешу әдістерін әзірлеу тарихқа бай. Төмендегі кестеде мұндай есептерді шешудің барлық әдістері мен модельдерін егжей-тегжейлі сипаттай отырып, барлық белгілі әдістерді жүйеледік. 1.3-кестеде ақпараттандыру объектісі үшін ақпараттық қауіпсіздік және киберқауіпсіздік көп контурлы жүйелерінің ұтымды конфигурацияларын табу есебін шешу үшін көп критерийліұтымды шешу әдістерінің салыстырмалы сипаттамасы келтірілген және ұтымды шешу есептерін шешу әдістерін салыстырмалы талдау жасалған.

№	Әдіс	Артықшылықтары	Кемшіліктері
1	2	3	4
1	Парето бойынша ұтымды шешімдер алу негізінде көп критерийлі келісімді қалыптастыру [47].	Әдісті практикада қолдану көп критерийлі ұтымды шешудің басқа әдістерімен салыстырғанда ең қарапайым болып табылады.	Зерттелетін параметрлердің маңыздылық деңгейін анықтау қиын. Ол үшін сарапшылардың сауалнамалары қолданылады, сондықтан бұл әдісті қолдану нәтижесі олардың субъективті енімдеріне байланысты болуы мүмкін.
2	Барлық басқа критерийтардың салмағын азайта отырып, бірнеше критерийтарды бір скаляр параметрге біріктіру [48].	Алынған параметрге жеке критерийтар тобының әсерін зерттеу қажет есептерді шешу үшін қолдануға болады.	Ұтымды шешімдерді іздеу ұтымды келісімге қол жеткізуге қандай критерийтар әсер ететіні белгісіз болғандықтан қиындайды және скаляр параметрінде критерийтарды өлшеу әдістерін анықтау қиын. Басқа критерийтардың салмағын азайту деңгейін анықтау қиын.

3	Өлшенген сомалар әдісі (басқалардың салмағын азайтпай бірнеше зерттелетін критерийларды біріктіру) [49].	Бұл әдісті бірнеше критерийтар бірдей мәнге ие есептерді шешу үшін қолдануға болады.	Әдісті қолдану нәтижесі есепті түрде ұтымды болмайды. Сонымен қатар, өлшенген коэффициенттерді анықтау қиын, олардың негізінде барлық критерийтар біріктіріледі.
4	Синтезделген «Парето нүктелері» әдісі және өлшенген сомалар әдісі [49, с.6].	Әдісті қолдану нәтижесі белгілі бір жағдайларда ең ұтымды «Парето нүктесі» болады.	Көп критерийліесепті шешуге субъективті аспект енгізетін сараптамалық бағалау әдісі қолданылады.
5	Мүлдем қолайсыз нұсқаға тыйым салу [50].	Бұл негізгі критерий бойынша нәтижені барынша арттыруға мүмкіндік береді.	Критерийтардың бірі қажетті талаптарға барынша сәйкес келмеген жағдайда ғана қолданылуы мүмкін.
6	Жүйелік көп критерийлі ұтымды шешу [52].	Максималды емес, керісінше есепті сәтті шешу ықтималдығын едәуір арттыратын ұтымды мәндерді іздеуге бағытталады.	Бұл әдіс сараптамалық сауалнама арқылы жүзеге асырылады. Бұл көп критерийлі есептерді шешуге субъективті аспектілік сипат береді. Егер сарапшылар ұтымды мәндердің қажетті аймағына сәйкес келетін параметр мәндерін таңдай алмаса, шешім табылмауы да мүмкін.
7	Операцияларды зерттеу әдістері [53].	Әдістердің қарапайымдылығы және барлық мүмкін баламаларды талдау мен салыстырудың салыстырмалы түрде қарапайым модельдері. Әдістер жақсы алгоритмделген. Бұл әдістер үшін жақсы танылған қолданбалы бағдарламалық қамтамасыз ету пакеттері бар.	Салыстыру параметрлері көбейген сайын, әдістер тиімділігін жоғалтады және күрделі тапсырмалар үшін әрдайым қолайлы бола бермейді.
8	Ойын теориясына негізделген әдістер	Ойындар теориясының математикалық	Көп критерийлі ұтымды шешу есептері үшін жоғары есептеу күрделілігі

	мен модельдер [54].	аппаратын қолданудың әмбебаптығы.	
9	Анық емес логика әдістері [54, 85 бет, 55].	Анық емес логикаға негізделген басқаруды ұтымды шешу әдістері көбінесе эвристикалық болып табылады.	Меншік функцияларын таңдауда және анық емес енгізу ережелерін қалыптастыруда субъективтілік бар, бұл әсіресе, көп критерийліұтымды шешу есептерін шешудің дәлдігіне әсер етеді.
10	Нейрожелілік [56].	Тәуелсіз айнымалылармен жұмыс істеу мүмкіндігі.	Тек ұтымды шешімдерді табуға мүмкіндік береді. Бұл әдістер әрқашан объектінің параметрлерін ұтымды шешу үшін жоғары дәлдікті қажет ететін тапсырмалар үшін қолданыла бермейді.
11	Интерактивті әдістер [57].	Әдістер жақсы алгоритмделген. Әдістер итерациялар жиынтығынан тұрады, олардың әрқайсысы шешім қабылдаушы тұлға жасаған талдау және есептеу кезеңдерін қамтиды.	Парето жиынын және/немесе алдыңғы жағын біркелкі жақындату үлкен есептеу шығындарын қажет етеді. Теңдестірілмейтін шешімдер санының артуымен қол жеткізілетін дәлдікке қойылатын талаптардың жоғарылауымен жалғыз шешімді таңдаумен байланысты есептер ұсынылған жиын шешім қабылдаушы тұлға үшін көп уақытты қажет етеді. Парето фронтының визуализациясында критерийтар саны екіден көп болған жағдайында қиындық бар.
12	Эволюциялық әдістер [58, 59].	Паретоның бүкіл алдыңғы жағын есептеуге мүмкіндік беретін көптеген шешімдер жасауға мүмкіндік береді.	Төмен жылдамдық пен Парето шешімдердің ұтымдылығына кепілдік берілмейді. Жасалған шешімдердің ешқайсысы шешімдердің басқа нұсқаларына үстемдік етпейтіні белгілі. Әдістер жаңа, дамуды қажет етеді.

Ұтымдылық критерийі бір (немесе бірнеше) [47-59] [60] ақпараттық (кибернетикалық) қауіпсіздік көрсеткіштері болуы мүмкін – ақпараттың қауіп-қатерлерін іске асырудан келтірілген залалдың шамасы, ақпараттың жайылып кетуінен болған залалды және оны қорғауға жұмсалған шығындарды, ақпаратты қорғауға жұмсалған инвестициялардан түскен пайданы, олардың рентабельділігін және тағы басқаларды қамтитын жалпы шығыстар.

Қойылған есептерді шешу бірқатар себептерге байланысты қиындайды. Ең бастысы, ұтымды шешімді іздеу тұрақсыздық жағдайында жүзеге асырылады, онда қарсыластың іс-әрекетін белгілі бір ықтималдықпен ғана болжауға болады, кейде тіпті мүмкін де болмайды. Қорғау құралдары мен әдістерінің әртүрлілігі, олардың сипаттамалары, қарсыласу схемаларының әртүрлілігі, қорғаныс жүйесінің жекелеген элементтерінің осалдықтарын дәл анықтау мүмкін еместігі, біздің елімізде статистикалық мәліметтердің болмауы да қолайлы әдістер тізіміне шектеулер қояды [61].

Жұмыстың басым есебі – ақпараттандыру объектісі көп тізбекті қорғаныс жүйелерінде және көп бағытты қарсыласу жүйелерінде ресурстарды ұтымды бөлудің адаптивті режимінде іздеу, мұнда тараптардың әрқайсысы өз ақпаратын сақтауға және қарсыластың ақпаратын алуға тырысады. Нақты объектілерге «байланыстырылған» жүйелердің кең класы үшін бұл есепті шешу көп контурлы ақпаратты қорғау құралдарының экономикалық және техникалық көрсеткіштерін жақсартуға мүмкіндік береді [62, 63]. Зерттеу объектісі үшін математикалық модельді құру бірнеше кезеңнен тұрады. Бірінші кезеңде мақсатты функцияны анықтап, ұтымды шешуге жататын көрсеткішті таңдау қажет. Мұндай көрсеткіштерге жүйенің сенімділігі, ақпараттың тарап кетуінен туындайтын залал, оны қорғауға жұмсалатын шығындар, ақпаратты қорғауға бөлінген ресурстар көлемі және олардың объектілер арасында бөлінуі, ақпаратты қорғауға салынған инвестициялардың рентабельділігі және басқа да параметрлер жатады. Екінші кезеңде мақсатты функция тәуелді болатын жүйенің параметрлері мен сипаттамаларын анықтау қажет. Үшінші кезеңде ақпаратты қорғау құралдары туралы мәліметтерді жинақтап, қарсы тұрудың ықтимал шарттарын анықтау керек. Мұнда объектілер бойынша ақпаратты бөлу, объектілердің осалдығының

қарсы тұру жағдайларына тәуелділігі, жекелеген объектілерге шабуыл жасалу ықтималдығы, сондай-ақ белгілі бір көлемдегі ресурстарды шабуылға бөлу ықтималдығы ескеріледі. Төртінші кезеңде мақсатты функцияның ақпаратты қорғау құралдарының параметрлері мен сипаттамаларына және қарсыласу жағдайларына тәуелділік сипатын, яғни функцияның формасын анықтау қажет. Бесінші кезеңде ұтымдылық критерийін таңдау керек. Ол ақпараттың тарап кетуінен болатын жиынтық залал, объектілер бойынша оның орташа мәні немесе әрбір объект үшін рұқсат етілетін ең жоғары мән болуы мүмкін. Есептеулерді ұйымдастыру келесі іс-шараларды қамтиды: есепті шешу әдісін таңдау, компьютерге арналған бағдарламаны құру және жөндеу, есептеулерді орындау, алынған нәтижелерді барынша ыңғайлы түрде ұсыну, сондай-ақ қорытындылар мен ұсыныстарды тұжырымдау.

1.3 IIoT және цифрлық егіздер жүйелеріндегі киберқауіпсіздікті зерттеудің академиялық аспектілері

Соңғы жылдары индустриялық Интернет заттары (IIoT) және цифрлық егіздер жүйелері ақпараттық қауіпсіздік саласында жаңа, күрделі мәселелерді тудырып отыр. Бұл технологиялар өндіріс пен өндірістік процестерді басқаруда маңызды рөл атқарады, өйткені сенсорлар, автоматтандыру элементтері және өндірістік бақылау жүйелері арқылы жиналған деректер нақты уақыт режимінде өңделеді. Мұндай деректер өндіріс тиімділігін арттыруға мүмкіндік бергенімен, олар ақпараттық қауіпсіздік тұрғысынан жаңа қатерлер мен осалдықтарды туындатады, себебі әртүрлі құрылғылар мен платформалардың бір-бірімен өзара әрекеттесуі қажет [99]. IIoT жүйелерінде қолданылатын деректерді жіберу протоколдары жүйенің сенімділігі мен өнімділігін тікелей анықтайды. Мысалы, MQTT over TCP ең төменгі кідіртуді қамтамасыз етеді, бұл өндірістік процестерде жылдам жауап қажет болған жағдайда маңызды болып табылады. Ал MQTT over WebSocket тұрақты кідіртуді көрсетеді, веб-қосымшалар мен таралған жүйелер үшін тиімді, ал HTTP протоколы кең үйлесімділік беретін болса да, кейде кідіртудің жоғары деңгейі мен тұрақсыздыққа ұшырайды [99]. Осы ерекшеліктер киберқауіпсіздік

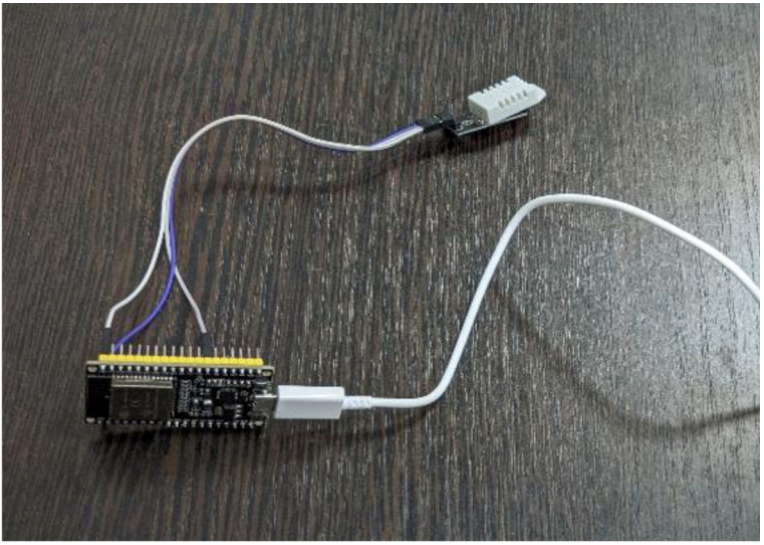
шараларын жобалауда және жүйелік сенімділікті қамтамасыз етуде протокол таңдау маңыздылығын дәлелдейді. Зерттеу ESP32-WROOM микроконтроллері мен DHT22 сенсорын қолданып жүргізілген. Деректерді жинау MQTT брокері (Mosquitto) арқылы жүзеге асырылды, ал HTTP үшін Python скрипті негізінде кідіріс өлшенді.

Кесте 1.4. Протоколдардың кідіріс статистикасы

Протокол	**Орташа (Mean), ms**	**Медиана, ms**	**Min, ms**	**Max, ms**	**SD, ms**
HTTP	342.6	289.9	47.8	2707.4	307.9
WebSocket	341.9	365.3	10.2	1982.5	193.2
MQTT over TCP	290.5	266.0	3.5	1992.5	325.7

1.4-кестеде үш түрлі протоколдың (HTTP, MQTT over TCP және MQTT over WebSocket) кідіріс көрсеткіштері салыстырылған. Нәтижелерге сәйкес, HTTP протоколы ең жоғары орташа кідірісті – 342.6 ms көрсетті. Сонымен қатар, оның стандартты ауытқуы да едәуір үлкен, бұл берілген протоколдың тұрақсыздығын және уақыт көрсеткіштерінің әртүрлі жағдайларда қатты өзгеріп отыратынын білдіреді.MQTT over WebSocket салыстырмалы түрде тұрақтырақ нәтижелер берді. Дегенмен, оның орташа кідіріс мәні HTTP протоколына жақын, яғни тиімділік тұрғысынан аса үлкен артықшылық бермейді. MQTT over TCP протоколы ең төмен орташа кідіріс – 290.5 ms көрсетті. Бұл оның жылдамдығы бойынша ең тиімді нұсқа екенін көрсетеді. Алайда дисперсиясы жоғары болғандықтан, сирек жағдайларда кідірістің ұлғаюы ықтимал. Жалпы алғанда, нәтижелер көрсеткендей, кідіріс тұрғысынан ең тиімді протокол – MQTT over TCP. Бірақ оның тұрақсыздық қаупін ескеру қажет, ал тұрақтылық маңызды болған жағдайда MQTT over WebSocket қарастырылуы мүмкін. HTTP болса, салыстырмалы түрде ең тиімсіз шешім ретінде бағаланады. Жалпы алғанда, реалды уақыттағы жауаптылық талап етілетін жүйелерде MQTT over TCP, ал веб-қосымшалар үшін MQTT over WebSocket тиімді болып табылады. HTTP болса, қарапайымдылығы мен үйлесімділігіне қарамастан, кідірісі жоғары болғандықтан,

нақты уақытты талап ететін IIoT жүйелеріне онша қолайлы емес [99].



1.12-сурет. ESP32 мен DHT22 негізіндегі эксперименттік конфигурация

Бұл суретте ESP32 микроконтроллері DHT22 сенсорына және қуат көзіне қосылған. Конфигурация деректерді жинап, оларды MQTT over TCP және MQTT over WebSocket протоколдары арқылы серверге жіберуге мүмкіндік береді. Мұндай орнату IIoT жүйелерінде кідіріс пен байланыс тұрақтылығын өлшеу үшін қолданылды. MQTT over WebSocket. Бұл протокол IoT жүйелерінде веб-қосымшалармен интеграцияға ыңғайлы. Алайда WebSocket инкапсуляциясы қосымша жүктеме енгізіп, кей жағдайда кідірісті арттырады. SSL/TLS шифрлауды қолдағанымен, веб-негізді шабуылдарға (XSS, CSRF) осал болуы мүмкін. MQTT over TCP. Бұл тәсіл ықшам әрі тиімді, қосымша жүктемесі аз. TCP арқылы берілетін деректер әдетте SSL/TLS арқылы қорғалады және IoT жүйелерінде кеңінен қолданылады. Орнатылуы оңай, сенімділігі жоғары.HTTP. HTTP хаттамасы кең таралған, қолдануға қарапайым және HTTPS арқылы сенімді байланыс қамтамасыз ете алады. Бірақ оның артық жүк-

темесі көп, себебі әрбір сұраныс жаңа қосылымды талап етеді. Сондықтан нақты уақыттағы IoT жүйелеріне тиімсіз[99]. Сонымен қатар, IIoT жүйелерінде деректерді жинау, сақтау және өңдеуге арналған аномалияларды анықтау жүйелерін дамыту мәселесі ерекше назар аударуды қажет етеді. [100] зерттеуде LSTM және CNN-LSTM нейрондық желілерін қолдану арқылы нақты уақыт режимінде аномалияларды анықтауға мүмкіндік беретін платформаны сипаттайды. Бұл тәсіл IIoT құрылғыларының шектеулі есептеу ресурстарына қарамастан жүйенің қауіпсіздігін қамтамасыз етуде тиімді. Архитектураның модульдік және бейімделгіш құрылымы әртүрлі өндірістік сценарийлерде қауіпсіздікті сақтау мен жаңа қатерлерге жылдам жауап беруді қамтамасыз етеді. Аномалияларды анықтау мақсатында ұсынылған әдісті оқыту және бағалау үшін синтетикалық IIoT (Industrial Internet of Things) деректері дайындалды. Бұл деректер қалыпты жұмыс жағдайларын және аномалиялық жағдайларды имитациялайды. Аномалиялар – сенсорлық мәндердегі кенеттен өсулер немесе ауытқулар, құрылғының ақаулары немесе киберқауіптің көрсеткіші ретінде қарастырылады.

Кесте 1.5 де Window Index бағаны белгілі бір ұзындықтағы уақыт терезелерінің қатарлы индексін көрсетеді, ал Labelбағаны осы терезеде аномалия бар екенін (1) немесе жоқ екенін (0) белгілейді [100].

Кесте 1.5. Сенсорлық деректердің терезелік көрінісінің мысалы

Терезе индексі	**Уақыт**	**Өлшеу мәні**	**Белгі (Mark)**
0	0.0	0.049671	0
1	0.1	0.006172	0
2	0.2	0.104758	0
3	0.3	4.810572	1
4	0.4	0.056499	0
5	0.5	0.076420	0
6	0.6	0.277633	0
7	0.7	0.216287	0
8	0.8	2.596473	1
9	0.9	0.233286	0

Алгоритм 1.1. ROC (Receiver Operating Characteristics) және AUC (Area Under Curve) метрикаларын есептеу

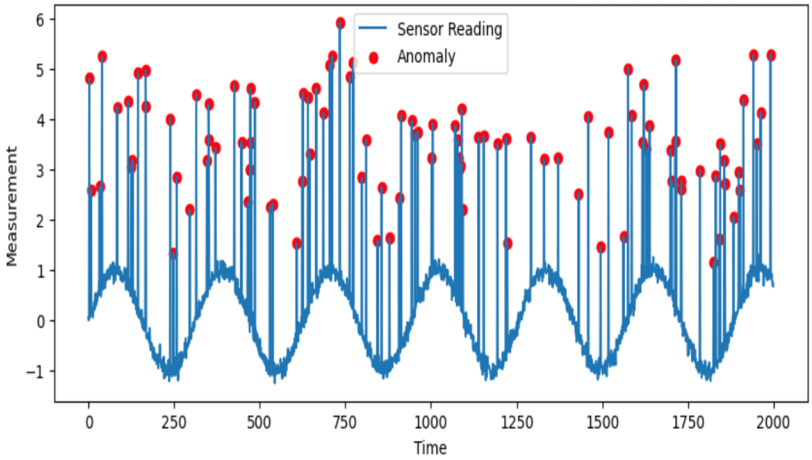
```
def generate_synthetic_iot_data(samples=2000, anomaly_frac=0.05, seed=42):
    np.random.seed(seed)
    time = np.arange(samples)
    signal = np.sin(0.02 * time) + np.random.normal(0, 0.1, samples)
    anomalies = np.random.choice(samples, int(samples * anomaly_frac), replace=False)
    signal[anomalies] += np.random.uniform(2, 5, len(anomalies))
        return pd.DataFrame({'time': time, 'measurement': signal, 'label': np.isin(time,
anomalies).astype(int)})

df = generate_synthetic_iot_data()

plt.plot(df['time'], df['measurement'], label='Sensor Reading')
plt.scatter(df[df['label'] == 1]['time'], df[df['label'] == 1]['measurement'], color='red',
label='Anomaly')
plt.title("Synthetic IIoT Sensor Data with Anomalies")
plt.xlabel("Time")
plt.ylabel("Measurement")
plt.legend()
plt.show()
```

Бұл алгоритм IIoT (Industrial Internet of Things) ортасында сенсорлық өлшеулерді модельдеу үшін синтетикалық уақыттық сериялар деректерін генерациялауға арналған. Оның жұмыс логикасы үш негізгі қадамнан тұрады.Біріншіден, негізгі сигнал генерациясы орындалады. Мұнда сенсордың қалыпты жұмысын бейнелеу үшін синусоидалық функция пайдаланылады: np.sin(0.02 * time). Бұл сенсор көрсеткіштерінің периодтық табиғатын көрсетеді. Дегенмен нақты өндірістік ортада өлшеулер әрқашан мінсіз болмайды, сондықтан алгоритм қосымша Гаусс шуын енгізеді: np.random.normal(0, 0.1, size=num_samples). Бұл шулар өлшеудегі кішігірім қателіктер мен табиғи флуктуацияларды имитациялайды. Екіншіден, аномалияларды енгізу және белгілеу жүзеге асырылады. Барлық деректердің шамамен 5%-ы кездейсоқ таңдалып, олардың мәндері күрт өсіріледі (np.random.uniform(2,5) аралығында). Мұндай шыңдар өндірістік сенсордың істен шығуын, техникалық ақауды немесе ықтимал кибершабуылды модельдейді. Әрбір уақыттық нүктеге екілік белгі беріледі: қалыпты жағдайға – 0, аномалияға – 1. Үшіншіден, алынған деректер негізінде модельді бағалау жүргізіледі. Ол үшін ROC (Receiver Operating Characteristic)

қисығы тұрғызылады. ROC нақты оң көрсеткіштерді (True Positive Rate) жалған оң көрсеткіштермен (False Positive Rate) салыстыруға мүмкіндік береді. Сонымен қатар, AUC (Area Under Curve) метрикасы есептеледі. Бұл көрсеткіш ROC қисығы астындағы ауданға тең және модельдің аномалияны ажырату қабілетін сипаттайды. Егер AUC мәні 1-ге жақын болса, модель жоғары дәлдікпен жұмыс істейді, ал 0.5 шамасындағы мән кездейсоқ болжаудан айырмашылығы жоқтығын білдіреді. Осылайша, бұл алгоритм сенсорлық деректердің шынайы сипаттамаларын ескере отырып, қалыпты режим мен аномалия жағдайларын қатар қамтитын синтетикалық мәліметтерді алуға мүмкіндік береді. Бұл мәліметтер кейін машиналық оқыту немесе жасанды интеллект модельдерін оқытуда, әсіресе IIoT киберқауіпсіздігі саласында, үлкен рөл атқарады.



1.13-сурет. Аномалиялары бар синтетикалық IIoT сенсорлық деректері

Сурет 1.13 синтетикалық IIoT сенсорлық деректерін көрсетеді, олардың ішінде аномалиялар бар. Matplotlib кітапханасы арқылы визуализация жасалған: қалыпты сенсорлық өлшеулер үздіксіз сызықпен бейнеленеді, ал аномалиялар қызыл нүктелермен ерекшеленеді. Бұл тәсіл аномалияларды тез және айқын анықтауға мүмкіндік береді[100]. Нейрондық желілер деректерден маңызды

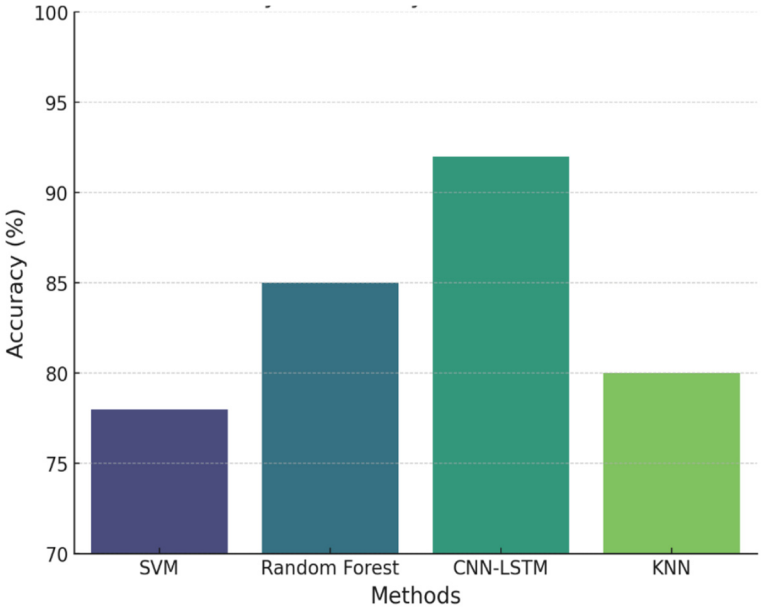
ерекшеліктерді шығару үшін өте тиімді болып табылады, әсіресе деректер көп өлшемді немесе шуды болған жағдайда. Мұндай әдістердің ішінде рекурренттік нейрондық желілер (RNN), оның ішінде Long Short-Term Memory (LSTM) архитектуралары уақыттық деректерді өңдеуге тиімді құрал ретінде танылған. Қосымша жетілдіру ретінде гибридтік CNN-LSTM модельдері қолданылады:

Конволюциялық қабаттар локалдық паттерндерді анықтайды;

Рекурренттік қабаттар ұзақ мерзімді тәуелділіктерді модельдейді.

Бұл құрылым күрделі уақыттық деректерде аномалияларды тиімдірек анықтауға мүмкіндік береді[100]. Аномалияларды анықтау үшін қолданылатын модельдер негізінен екі түрге бөлінеді. LSTM моделі бір немесе бірнеше LSTM қабатынан құралады және соңында бинарлы классификацияға арналған тығыз қабат қосылады. Бұл тәсіл уақыттық тәуелділігі жоғары сигналдарды талдауға ыңғайлы, сондықтан сенсор деректеріндегі ұзақ мерзімді динамика мен трендтерді тиімді модельдейді. CNN-LSTM моделі алдымен конволюциялық қабаттар арқылы деректерден локалдық үлгілерді бөліп алады, бұл кенеттен пайда болатын қысқа мерзімді аномалияларды анықтауға көмектеседі. Кейін LSTM немесе GRU қабаттары уақыт бойынша тәуелділікті біріктіріп, толық суретті қалыптастырады, сондықтан бұл тәсіл күрделі әрі тұрақсыз деректер ағындарында нәтижелі болып келеді. Модельді дайындау және бағалау процесі бірнеше негізгі қадамнан тұрады. Алдымен алдын ала өңделген уақыттық сериялар оқу, валидация және тест жиынтықтарына бөлінеді, бұл модельдің жалпылау қабілетін тексеруге мүмкіндік береді. Содан кейін модельдің конфигурациясы жасалып, LSTM блоктарының саны, жасырын қабаттардың тереңдігі, оқу жылдамдығы мен пакет мөлшері сияқты гиперпараметрлер анықталады. Оқыту кезеңінде Adam немесе RMSProp секілді оптимизаторлар қолданылады, ал шығын функциясы ретінде бинарлы кросс-энтропия алынады. Әрбір эпоха барысында оқу және валидация нәтижелері бақылауда болады. Егер бірнеше эпох бойы валидация көрсеткіштері жақсармаса, оқытуды ерте тоқтату тәсілі қолданылады. Бұл артық үйренудің алдын алып, есептеу ресурстарын үнемдейді. Осы тәсілдердің

нәтижесінде модель қалыпты және аномальды уақыттық деректерді ажырата алатын қабілетке ие болады, ал архитектураның таңдауы нақты қолдану жағдайына байланысты анықталады. Әрбір эпохта модель өз параметрлерін кезең-кезеңімен жетілдіреді, бұл аномалиялық деректерді қалыпты сегменттерден тиімді ажырата алуға мүмкіндік береді. Осындай итеративті оқыту процедурасы өндірістік процестерді күтпеген ақаулардан қорғайтын сенімді және проактивті аномалияларды анықтау жүйесінің негізін құрайды[100].



1.14-сурет. Аномалияларды анықтау әдістерінің дәлдігі

Сурет 1.14 әртүрлі CNN-LSTM әдістерінің дәлдігін (%) салыстырады. Нәтижелер көрсеткендей, CNN-LSTM гибридтік моделі ең жоғары дәлдік (~92%) көрсетіп, ең тиімді әдіс болып табылады.

Random Forest әдісінің дәлдігі шамамен 85%, бұл оны жақсы балама етеді.

KNN орташа дәлдік (~80%) көрсетеді, жұмыс істейді, бірақ басқа модельдерге қарағанда әлдеқайда төмен.

SVM ең нашар дәлдік (~78%) көрсетеді, бұл оның осы тапсырма үшін тиімді еместігін білдіреді[100].

Кесте 1.6. Ұсынылған IIoT архитектурасы мен дәстүрлі шешімдер арасындағы негізгі айырмашылықтар

Критерий	**Дәстүрлі IIoT архитектуралары**	**Ұсынылған IIoT архитектурасы**
Қауіпсіздік әдістері	Негізгі аутентификация әдістері, қарапайым шифрлау	RBAC, AES-256, TLS/SSL, Атака анықтау жүйесі (IDS/IDPS)
Аномалияларды анықтау	Қарапайым ережелер немесе статистикалық әдістер	CNN-LSTM гибридтік моделі, адаптивті оқытумен
Ресурстарға тәуелді ортаға бейімделу	Жоғары есептеу қуатын талап етеді	Edge AI арқылы модельді қысқарту әдістері
Энергия тұтыну	Бұлтта деректерді үнемі өңдеу нәтижесінде жоғары	Деректерді оңтайлы тасымалдау, таралған есептеу арқылы энергия үнемдеу
Масштабталу	Шектеулі, орталық серверлерге тәуелді; жүктеме артқанда кідірістер пайда болады	Edge AI және таралған деректерді өңдеу арқасында жоғары өнімділік, бұлттағы жүктемені азайтады

Ұсынылған IIoT архитектурасы RBAC, AES-256, TLS/SSL және IDPS арқылы дәстүрлі шешімдермен салыстырғанда айтарлықтай жоғары қауіпсіздікті қамтамасыз етеді. Қарапайым статистикалық әдістерден айырмашылығы, CNN-LSTM гибридтік моделі аномалияларды дәлірек және жылдамырақ анықтауға мүмкіндік береді, сонымен қатар өзгеретін жағдайларға бейімделеді. Edge AI және модельді қысқарту әдістерін пайдалану есептеу процестерін оңтайландырады, бұл бұлт ресурстарына жүктемені азайтып, жүйені икемдірек әрі энергия тиімді етеді. Нәтижесінде, жаңа

архитектура өндірістік IIoT үшін сенімді, бейімделгіш және масштабталатын шешім ұсынады[100].

Кесте 1.7. Модельдердің өнімділік параметрлерін салыстыру (жауап беру уақыты, дәлдік, қуат тұтыну).

Модель	**Жауап беру уақыты (мс)**	**Дәлдік (%)**	**Қуат тұтыну***
CNN-LSTM	15 ± 2	~92	Орташа–Жоғары
Random Forest	10 ± 3	~85	Жоғары
KNN	5 ± 1	~80	Орташа
SVM	8 ± 2	~78	Төмен

Қуат тұтыну көрсеткіштері шартты, нақты CPU/GPU түріне байланысты.

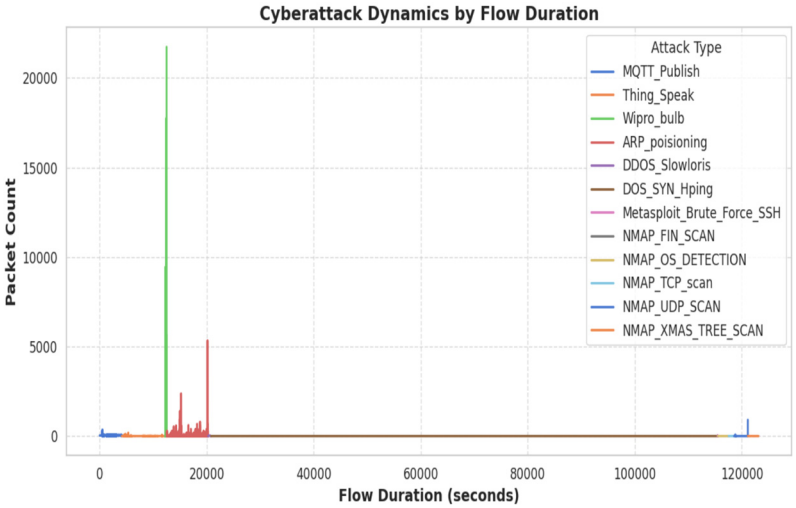
Кесте 1.8. Дәстүрлі мониторинг жүйелері мен ұсынылған архитектураны салыстыру.

Критерий	**Дәстүрлі жүйелер**	**Ұсынылған архитектура (CNN-LSTM + көпдеңгейлі қорғау)**
Қауіпсіздік әдістері	Қарапайым аутентификация, дерекқорлар	RBAC, AES-256, TLS/SSL, IDPS
Аномалияны анықтау	Статистикалық шектер/ережелер	CNN-LSTM гибридті моделі
Шектеулі ресурстарға бейімделу	Масштабтау қиын	Модельді қысу, Edge AI
Жауап беру жылдамдығы	Орташа	Жоғары (төмен кідіріс)
Масштабталу	Шартты түрде шектеулі	Жоғары (таратылған түйіндер)
Кибершабуылдарға төзімділік	Төмен–Орташа	Жоғары (IDS, көпдеңгейлі қорғау)

Сонымен бірге, IIoT инфрақұрылымындағы кибершабуылдардың динамикасын талдау мақсатында жүргізілген зерттеулер (Adilzhanova, Kunelbayev, Amirkanova, Tyulepberdinova, Sybanova, 2025) машиналық оқыту алгоритмдерін пайдалана отырып шабуылдардың әртүрлі типтерін классификациялаудың тиімділігін көрсетті [101]. Random Forest моделі деректерді өңдеуде ең жоғары

дәлдікке жетіп, сирек кездесетін шабуыл түрлерін де сенімді анықтады.

Зерттеу барысында авторлар деректер теңгерімсіздігі мәселесін шешу үшін кросс-валидация және теңестіру әдістерін қолдануды ұсынды. Бұл тәсілдер IIoT қауіпсіздік жүйесінің нақты уақыттағы өнімділігін арттырып, сирек кездесетін кибершабуылдарды жіберіп алмауға мүмкіндік береді. Жүргізілген жұмыстардың нәтижелері IIoT және цифрлық егіздер жүйелерінде киберқауіпсіздікті қамтамасыз ету үшін кешенді, көпқырлы тәсілдің қажеттілігін айқындады. Мұндай тәсіл дұрыс коммуникациялық протоколдарды таңдауды, деректерді қорғаудың адаптивті алгоритмдерін енгізуді, нейрондық желілер арқылы аномалияларды анықтауды және машиналық оқыту әдістерін пайдалана отырып шабуыл түрлерін классификациялауды қамтиды. Осындай интеграцияланған шешімдер жүйелердің сенімділігін арттырып, ақпараттық шығындарды азайтады және жаңа кибершабуылдар мен аномалияларға қарсы бейімделгіш қорғаныс қабілетін қамтамасыз етеді.



1.15-сурет. Flow Duration динамикасы

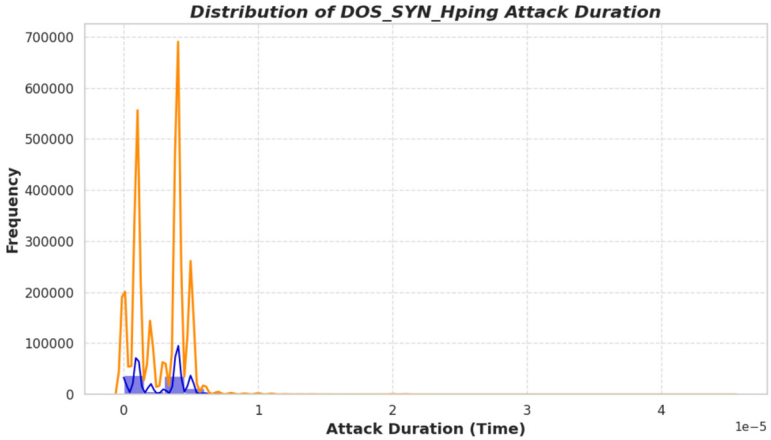
Әрбір шабуыл түрі үшін Seaborn және Matplotlib кітапханалары арқылы сызылған сызықтық график берілген. Графикте ағын

ұзақтығы мен пакеттер саны арасындағы өзара байланыс көрсетілген.

Кесте 1.9. IIoT шабуылдарын классификациялау модельдерінің нәтижелері

Модель	**Cross-validation қолданылмаған**	**Cross-validation қолданылған**
Logistic Regression	77.07 %	99.10 %
Random Forest	99.65 %	99.82 %
K-Nearest Neighbors (KNN)	99.13 %	99.59 %

Бұл 1.9. кестеде үш машиналық оқыту моделі (Logistic Regression, Random Forest және KNN) IIoT шабуылдарын классификациялауда қолданылған. Cross-validation әдісі қолданылғанда барлық модельдердің дәлдігі артты, ал ең жоғары нәтижені Random Forest көрсетті (99.82 %)[101].



1.16-сурет. DOS_SYN_Hping шабуылының ұзақтығының үлестірімі

Бұл 1.14. суретте уақытқа байланысты желі ағынының ұзақтығы көрсетілген. Максималды мән арнайы белгіленіп, шабуыл кезіндегі трафик динамикасын визуалды бақылауға мүмкіндік береді. Жалпы, алдағы зерттеулер IIoT инфрақұрылымын қорғауда заманауи машиналық және терең оқыту әдістерін қолдануға бағытталады.

Бұл қауіпсіздік жүйелерінің дәлдігі мен бейімделгіштігін арттырып, жаңа қауіптерге төтеп беру қабілетін күшейтеді.

1.4 1-тарау бойынша қорытындылар.

Қазіргі заманғы ақпаратты қорғау құралдары – бұл өте күрделі құрылымдар, олар көп тізбекті киберқауіпсіздік жүйелерінің қорғауында болатын көптеген объектілерді қамтуы мүмкін. Аппараттық, бағдарламалық, ұйымдастырушылық құралдар мен қорғаныс әдістерінің әртүрлі конфигурацияларын қамтуы мүмкін мұндай жүйелерді зерттеу қиын есеп болып табылады. Мұндай есептерді, соның ішінде, математикалық модельдеудің әртүрлі әдістерін және ақпараттандыру объектісі көп контурлы қорғаныс кешендерінің құрамын көп критерийлі ұтымды шешуді қолдана отырып шешуге болады. Жоғарыда айтылғандарды ескере отырып, жұмыстың бірінші тарауында келесі негізгі нәтижелер алынды және монографиялық зерттеудің келесі тарауларында шешуді қажет ететін есептер белгіленді. ISO / IEC TR 13335 сәйкес ақпараттық-коммуникациялық технологиялар сегменті ретінде ақпараттық-коммуникациялық жүйе қауіпсіздігін басқару модельдері талданды. ISO / IEC 27001:2010 стандартына сәйкес «жоспарла – орында – тексер – әрекет ет» моделінің мазмұны ашылды. Ақпараттандыру объектісі, ақпараттық қауіпсіздік және оның ақпараттық-коммуникациялық жүйе басқару құрылымы ақпараттың өмірлік циклі деңгейінде «объект – қауіп – қорғау» тұжырымдамасына және «кибернетикалық кеңістік – коммуникациялық орта – физикалық кеңістік» көп деңгейлі моделіне сәйкес талданды. Бұл тәсіл ақпараттық-коммуникациялық жүйені басқару құрылымында көп деңгейлі қорғау элементтерін барабар таңдауға, ақпараттық ресурс құпиялылығын, тұтастығы мен қолжетімділігін қамтамасыз етуге, сондай-ақ қорғау тараптарының ресурстарын адаптивті басқару жөніндегі есептерді шешуге мүмкіндік береді. Қолданыстағы ақпаратты қорғау құралдары ұтымды шешу модельдерін талдау көрсеткендей, қарастырылған модельдердің көпшілігінің мақсаты ақпараттық қауіпсіздікке жалпы шығындарды оңтайландыруға бағытталған (Гордон-Леб моделі, К. Задираки моделі). Тек жекелеген модельдер ғана (мысалы, Глушак-Новиков моделі) адаптивті режимде ақпараттық қауіпсіздік объектілері арасында ұтымды

қаражат бөлуді іздеуге бағытталған. Осы ғылыми нәтижелерді негізге ала отырып, IIoT (Industrial Internet of Things) және цифрлық егіздер жүйелеріндегі киберқауіпсіздікті зерттеу аспектілері ерекше мәнге ие болып отыр. Себебі IIoT құрылғыларының көптігі, олардың әртүрлі протоколдар арқылы өзара әрекеттесуі, сондай-ақ нақты уақыттағы деректер алмасуы жаңа осалдықтар мен киберқауіптерді тудырады. Зерттеу нәтижелері мынадай маңызды тұжырымдар жасауға мүмкіндік берді. Протоколдарды дұрыс таңдау IIoT ортасында шешуші рөл атқарады: MQTT over TCP нақты уақыт жүйелері үшін тиімді, MQTT over WebSocket веб-қосымшаларға қолайлы, ал HTTP жоғары кідірісі себебінен IIoT үшін жарамсыз деп бағаланды [99]. LSTM және CNN-LSTM негізіндегі нейрондық желілер сенсорлық деректердегі аномалияларды дәлірек тануға мүмкіндік берді, соның ішінде CNN-LSTM моделі шамамен 92% дәлдік көрсетті [100]. Машиналық оқыту алгоритмдерінің ішінде Random Forest шабуыл түрлерін жіктеуде ең жоғары нәтижеге жетіп, 99.82% дәлдік көрсетті және сирек кездесетін шабуылдарды да тиімді анықтай алды [101]. Edge AI, RBAC, TLS/SSL және IDS/IDPS біріктірілген жаңа архитектура дәстүрлі шешімдерге қарағанда сенімдірек, бейімделгіш әрі энергия тиімді жүйе құруға мүмкіндік беретіні дәлелденді. Жалпы алғанда, бұл тараудың қорытындылары IIoT және цифрлық егіздер жүйелерінде қауіпсіздікті қамтамасыз ету үшін кешенді, интеграцияланған тәсілдің маңыздылығын көрсетті. Мұндай тәсіл дұрыс протоколдарды таңдауды, адаптивті қорғаныс алгоритмдерін енгізуді, нейрондық желілер негізінде аномалияларды анықтауды және машиналық оқыту арқылы шабуылдарды классификациялауды қамтуы тиіс.

2 ҚОРҒАУ ОБЪЕКТІЛЕРІ АРАСЫНДА РЕСУРСТАР-ДЫ БӨЛУДІ ОҢТАЙЛАНДЫРУ

2.1. Теориялық және ойын әдістері негізінде ақпараттық ресурстарға шабуыл жасау және қорғаныс тараптарының қарсылығын модельдеу

Белгісіздік жағдайында тиімді ақпаратты қорғау құралдары құру үшін маңызды есеп-қорғаныс объектілері арасында ресурстарды бөлудің мүмкін нұсқаларын зерттеу және олардың ішінен оңтайлысын таңдау. Қорғау тарапының мақсаты - қауіп-қатерлердің ықтималдығын азайту. Шабуыл жағы тікелей қарама-қарсы мақсаттарды көздейді. Шабуыл жасаушылар өз ресурстарын киберқауіптерді іске асырудан барынша тиімділікке қол жеткізетіндей етіп бөлуі тиіс. Шын мәнінде, бұл жағдай ойын теориясының есепін қоюға қатысты [65, 66, 67]. Әр тараптың жеңісі қарсыластың стратегиясына байланысты және $o(h,d)$. мақсатты функциямен анықталады.

Мұнда жоғарыда тұжырымдалған тұжырымдағы есеп нөлдік сомадағы ойынның асимметриялық жағдайына сәйкес келетіндігін нақтылау қажет. Яғни, бірінші ойыншы ғана жеңе алады (шабуылдаушы (h хакер)). Оның ұтысы залал келтірілген ақпараттық ресурс құнымен бағаланады. Содан кейін қорғаныс жағының d жоғалуы шабуылдаушының жеңісіне тең.

Мұндай есептерді қою үшін әр тарап (h,d) өзінің жеңіс функциясын біледі деп болжаймыз. Сондай-ақ, әр тараптың өз мақсаттарын іске асыру үшін бірқатар стратегиялары бар.

Жоғарыда айтылғандай, тараптардың әрқайсысының өз есептерін орындау үшін өз ресурстары болады. Тиісінше, шабуылдаушылардың H ресурстары бар. Қорғау жағында D ресурстар бар. Ресурстар саны шектеулі және әртүрлі нысандарға бағытталуы мүмкін.

Шабуылдаушы (шабуылдаушылар) стратегиясы - өз ресурстарын объектілер арасында әртүрлі арақатынаста бөлу:

$$\{h_{ik}\} = (h_1, h_2, ..., h_l), \sum_{k=1}^{l} h_k = H, h_k \geq 0, \qquad (2.1)$$

мұнда, k - қорғау объектісінің нөмірі $\left(k = \overline{1,l}\right)$, h_k - объектіде қатерлерді іске асыруға арналған шығындар (ресурстар).

Сол сияқты, қорғаныс жағы ресурстарды бөлудің өзіндік стратегиясын қолданады:

$$\left\{d_{jk}\right\} = \left(d_1, d_2, ..., d_l\right), \sum_{k=1}^{l} d_k = D,\ d_k \geq 0, \qquad (2.2)$$

мұнда, d_k k-объектіде қорғауды іске асыруға арналған шығындар (ресурстар).

Шабуылдың шыңында шабуылдаушы қорғаныс жағына көп зиян келтіруге тырысатындықтан, мақсатты функцияны келесідей беруге болады:

$$o\left(h_k, d_k\right) \to \max. \qquad (2.3)$$

Келтірілген залалдың мөлшерін ақпараттық ресурс немесе ақпараттық инфрақұрылымның құнымен бағалауға болады. Залал мөлшері тараптардың ресурстарын бөлуге байланысты болады.

Қорғаныс жағы қарсы мақсатқа ұмтылады. Қорғау қауіптерді жүзеге асыру нәтижесінде келтірілген зиянның мөлшерін азайту керек. Демек, жалпы жағдайда қорғаныс жағы үшін мақсатты функция келесідей берілуі мүмкін:

$$o\left(h_k, d_k\right) \to \min. \qquad (2.4)$$

Теориялық және ойын тәсілін қолдана отырып, келесі кезеңде бағандар қорғаныс ресурстарын бөлу нұсқаларына $\left\{d_{jk}\right\}$, ал жолдар шабуыл ресурстарын бөлудің ықтимал нұсқаларына $\left\{h_{ik}\right\}$ сәйкес келетін функция $o\left(h_k, d_k\right)$ үшін жеңіс матрицасы жасалады. Осылайша, мынаны аламыз:

$$o = \begin{pmatrix} o_{11} & o_{12} & \ldots & o_{1n} \\ o_{21} & o_{22} & \ldots & o_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ o_{m1} & o_{m2} & \ldots & o_{mn} \end{pmatrix}, \qquad (2.5)$$

мұнда, o_{ij} – қауіптерді іске асырудан келтірілген зиянның мөлшері. Ойыншылардың таза стратегияларын қолдану мүмкіндігі үшін $\left(i = \left(\overline{1,m}\right),\ j = \left(\overline{1,n}\right)\right)$

Осы матрицалық ойынның қажетті стратегиясы қорғаныс жағының ресурстарын оңтайлы бөлу болып табылады.Оңтайлы стратегияны іздеген кезде қорғаныс жағы *j*-ші бағанды таңдайды деп болжап, шабуыл жағы *i*-ші жолды қарастырады. Бұл жағдайда жеңіс o_{ij} – элемент болады. Тараптардың мүдделері диаметрлік қарама-қарсы. Ойыншылардың әрқайсысы қарсыластың стратегиясын білмейді. Бұл тараптардың шешім қабылдауын қиындатады.

Егер ойыншылардың әрқайсысы 1 ықтималдығымен белгілі бір стратегияны таңдаса, онда олар таза стратегияны қолданады деп саналады. Бұл жағдайда ойын шешімі таза стратегияларда болады [68]. Ойынның шешімі - әр ойыншының оңтайлы стратегиясын анықтау болып табылады. Егер осы стратегияны қолдану басқа ойыншының барлық мүмкін стратегиялары үшін ең үлкен кепілдендірілген жеңісті қамтамасыз етсе, онда ойыншының стратегиясы оңтайлы болады [68]. Осыған сүйене отырып, шабуылшы жеңіс матрицасын (2.5) осылай зерттейді. Әрбір *i*-жолда $\left(i=\overline{1,m}\right)$ қорғау стратегиясын таңдауға байланысты o_{ij} ұтыстың ең аз мәні анықталады $\min\limits_{j} o_{ij}$., яғни шабуылдаушылардың өзінің *i*-таза стратегиясын қолдану нұсқасы үшін қауіпті іске асыру нәтижесінде келтірілген залалдың ең аз мәні анықталады. Ең төменгі ұтыстардың $\min\limits_{j} o_{ij}$ ішінде біз осы ең төменгі ұтыстың максималды болатын *i*-стратегиясын анықтаймыз. Сондықтан ойынның төменгі бағасын $\alpha=\max\limits_{i}\min\limits_{j} o_{ij}$ табу керек. Қорғаныс жағы симметриялы әрекет етеді. Қорғаныс жағы үшін біз ойынның жоғарғы шекарасын табамыз, ол қауіп-қатер туындаған жағдайда шабуылдаушының ең көп зиян келтіруі мүмкін екенін көрсетеді. Жоғарғы шекара ойындар үшін тараптар қорғауын осылайша табамыз: $\beta=\min\limits_{j}\max\limits_{i} o_{ij}$

Егер ойында жоғарғы және төменгі шекаралар сәйкес келсе, онда ойынның ершік нүктесі болады. Яғни $\max\limits_{i}\min\limits_{j} o_{ij}=\min\limits_{j}\max\limits_{i} o_{ij}=\Psi$ болады. ψ – ойын бағасы. Бұл жағдайда $\max\limits_{i}\min\limits_{j} o_{ij}$ шабуылдаушылар және $\min\limits_{j}\max\limits_{i} o_{ij}$ қорғаныс

жағы үшін ойыншылардың таза стратегиялары оңтайлы болады. Шабуылдаушының стратегиясы оңтайлы стратегиядан ауытқыған кезде оның пайдасы азаяды. Сол сияқты, қорғаныс жағы өзінің оңтайлы стратегиясынан сәл ауытқып, қауіптерді іске асыру нәтижесінде туындауы мүмкін зиянның мөлшері артады.

Егер ершік нүктесі жоқ болса, онда ойынның төменгі және жоғарғы бағаларының табылған мәндері қорғаныс жағының жоғалуы ойынның жоғарғы бағасынан аспайтындығын және кем дегенде ойынның төменгі бағасына тең болатындығын көрсетеді. Ойыншылардың таза стратегиялары оңтайлы нәтиже бермейтіндіктен, ойын теориясы аралас стратегияларды қолдануды ұсынады [68, с. 170].

Шабуылдаушылардың аралас стратегиялары $W_H^0 = (P_1,..., P_m)$ ықтималдықтар жиынтығымен берілген. Ойыншы бастапқы таза стратегияларын қолданады $\{h_i\}\left(i = \overline{1,m}\right)$ және $\sum_{i=1}^{n} P_i = 1,\ P_i \geq 0,\ i = \overline{1,m}.$

Сол сияқты, аралас стратегиялар қорғаныс жақтары өздерінің ықтималдық жиынтығымен берілген:

$$W_D^0 = (Q_1,..., Q_n): \quad \sum_{j=1}^{n} Q_j = 1,\ Q_j \geq 0,\ j = \overline{1,n}. \quad o^0 = \sum_i \sum_j P_i Q_j o_{ij}. \quad (2.6)$$

[69, 70] Көрсетілгендей ойынның шешімі сызықтық бағдарламалау есебін шешуге дейін әкеледі.

Оңтайлы аралас стратегияның S_D^0 қасиеті бар, оған сәйкес қорғаныс жағының жеңілісі шабуылдушылардың кез келген мінез-құлықтағы ойын бағасының $\psi -$ мәнінен аспайды.

$\psi -$ ойын бағасының мәні алдын-ала белгісіз. Бірінші кезеңде $\psi > 0$ деп санауға болады(бұл үшін o_{ij} барлық элементтердің оң болуы жеткілікті).

Егер қорғаныс жағы аралас стратегияны қолданса және өзінің *i*- таза стратегиясына шабуыл жасаса, онда зиянды математикалық күту келесідей анықталады: $o_i = o_{i1}Q_1 + o_{i2}Q_2 + ... + o_{in}Q_n$. Ресурстарды бөлу есептерін, оның ішінде қорғаныс жағының ресурстарын адаптивті бөлу есептерін шешкен кезде, ең алдымен, ақпараттық қауіпсіздік объектілері арасында оңтайлы бөлуді іздеу моделінің мақсат функциясын қалыптастыру қажет.

Осыған байланысты, ресурстар туралы айтқанда, бірінші кезеңде ресурс дегеніміз, ең алдымен, қорғаныс объектілері арасында бөлінуі керек қаржылық ресурстарды білдіреді деп болжауға болады, 2.1-суретті қараңыз. 2.1-суретте қызметкерлер мен клиенттердің дербес деректерін; аумақты, ғимараттар мен үй-жайларды, деректерді беру желілерінің серверлері мен автоматтандырылған жұмыс орындарын; технологияларды (электрондық түрдегі ақпарат, технологиялық процестердің құрылымы); қаржылық қызмет туралы деректерді және т. б. қорғауға жіберу қажет ресурстарды бөлудің (шартты кәсіпорындар үшін) мысалы көрсетілген.

2.1-сурет. Әртүрлі қорғау объектілеріне жұмсалған қаржы ресурстарын бөлу нұсқасының мысалы

Әрине, ресурстарды бөлуді қажет ететін ақпараттық қауіпсіздік объектілерінің тізімі өзгеруі мүмкін және компанияның немесе кәсіпорынның бизнес-процестерінің ерекшелігіне байланысты болады. Банк, өндіріс немесе білім беру саласындағы қорғау объектілері әртүрлі, сондықтан ресурстарды (ең алдымен, қаржылық) әмбебап модельді қолдана отырып бөлу қиын. Сондай-ақ, ресурстарды бөлу туралы айтқанда, қазіргі заманғы қорғаныс жүйелерінің ерекшеліктерін ескеру қажет екенін есте сақтаған жөн. Мысалы, көптеген компаниялар шабуылдаушылар үшін тұзақтарды қолдана бастады [71]. Бұл технологиялар компаниялар-

дың немесе кәсіпорындардың арнайы, параллель желілеріне негізделген. Бұл желілерде тапсырыс берушінің IT-инфрақұрылымына таралған жасырын желілік тұзақтар мен жемдер орнатылады. Шабуылшылардың ресурстарын мұндай қайта бөлудің барлау немесе тарату сатысында шабуылдарды анықтауға көмектесу ықтималдығы өте жоғары.

Ресурстарды бөлу немесе қайта бөлу туралы айтатын болсақ, біз оңтайландыру көп критерийлі есеппен айналысамыз. Мұндай есептерді шешу барысында көбінесе арнайы мақсатты функцияларды қолдану қажет. Мұндай функциялар көбінесе сызықты емес және унимодальды емес. Сонымен қатар, мұндай функциялардағы шектеулер сызықты емес және дөңес емес. Мұндай көп критерийлі оңтайландыру есептеріндегі айнымалылар және ақпараттық қауіпсіздік объектілері арасындағы оңтайлы үлестіруді іздеу моделінің мақсатты функциялары үздіксіз, тұтас, логикалық, аралас болуы мүмкін [72, 73].

Көптеген мұндай көп критерийлі оңтайландыру есептерін шешудің дәстүрлі стратегияларын іске асыру айтарлықтай есептеуді қажет етуі мүмкін. Айта кету керек, табылған шешім өзекті болып табылатын және нәтиже ақпараттық ресурсты жоғалту қаупі тұрғысынан қолайлы болатын уақыт аз болады. Шабуыл жасаушылар шабуыл техникасын үнемі жетілдіріп отырады, сондықтан жағдай үнемі өзгеріп отырады және үнемі жаңа шешімдерді талап етеді. Мұндай жағдайларда оңтайландыру есептерін шешудің генетикалық алгоритмдері ерекше қызығушылық тудырады. Алайда, қорғау тарапының ресурстарын адаптивті бөлу есебін шешу үшін генетикалық алгоритмді әзірлеуге кіріспес бұрын, ақпараттық қауіпсіздік объектілері арасында ресурстарды бөлудің мақсатты функциясын қалыптастыру керек. Белгілі бір ақпараттық жүйенің математикалық моделін жасау кезінде мақсатты функцияға кіретін параметрлердің мәндерін және тәуелділік формасын анықтау қажет [74]. Анықталған кемшіліктерді жою және ақпаратты қорғау құралдары модельдеу саласындағы соңғы жетістіктерді пайдалану мақсатында ақпараттық қауіпсіздіктің қолданыстағы модельдеріне бірінші тарауда жүргізілген талдау негізінде мақсатты функцияның негізгі компоненттері анықталды. Таңдалған модель үшін мақсатты функция қауіптерді іске асырудан келтірілген залалды білдіреді және түрі осылай болады [75]:

$$o(h_k, d_k) = \sum_{k=1}^{l} o_k(h_k, d_k) = \sum_{k=1}^{l} g_k p_k v_k(h_k, d_k), \quad (2.7)$$

Мұндағы $k = \overline{1,l}$ – қорғауға арналған объектінің нөмірі;

h_k, d_k – тиісінше, қорғаныс шабуылының ресурстары;

g_k – ақпараттық қауіпсіздік *k*-объектісіндегі ақпараттық ресурс салыстырмалы мәні;

p_k – ақпараттық қауіпсіздік объектісіне шабуыл жасау ықтималдығы;

$v_k(h_k, d_k)$ – ақпараттық қауіпсіздік *k*-объектісінің осалдығы. Осалдық шабуылдаушылар мен қорғаныс жақтарының ресурстарының арақатынасына байланысты.

$o(h,d)$, $o_k(h,d)$, g_k шамалар ақпараттық ресурстың барлық құнына жатады. $v_k(h_k, d_k)$ – мән талданатын объектідегі ақпараттың құнына жатады. Қарама-қайшылық белгісіздік жағдайында қарастырылады. Шын мәнінде, киберқақтығыстардың нақты тәжірибесіндегідей, p_k шабуылдың ықтималдығын бағалау мүмкін емес. Сондықтан біз $p_k = 1$, яғни (шабуыл болды) деп санаймыз.

Объектінің $v(h,d)$ осалдығы сәтті шабуылдың ықтималдығы ретінде қарастырылады және шабуылдаушылардың шығындары мен нысанды қорғау шығындарына байланысты. Бірінші кезеңде мақсатты функцияға кіретін параметрлердің мәні мен тәуелділік формасын табу керек. Объектілердегі g_k ақпараттың салыстырмалы құндылығын дәл анықтауға болады. Объектілерге p_k шабуыл жасау ықтималдығы мен $v(h,d)$ тәуелділік формаларын анықтау тараптардың тактикасының белгісіздігімен күрделене түсетін маңызды есеп болып табылады.

Тапсырма екі бағыт бойынша орындалды. Бірінші бағыт ақпаратты қорғау құралдары көрсеткіштерін енгізу: Қорғау объектілерінің саны; Объектілердегі g_k ақпараттың салыстырмалы құндылығы; Оның табиғи қорғалуымен айқындалатын объектінің бастапқы $v(h,0)$ осалдығы; Қорғау ресурстарының

жалпы саны – $D=\sum_{k=1}^{l} d_k$; 5) қалдық тәуекел. Қарсыластың іс-қимылын бағалау: Шабуылдардың сипаты (олардың бағытталуы мен қарқындылығы); Объектілерге p_k шабуыл жасау ықтималдығы; Шабуыл жасау ресурстарының жалпы саны - $H=\sum_{k=1}^{l} h_k$; Шабуыл жасаушылардың $\{h_k\}$ ресурстарын объектілер бойынша ықтимал бөлу. Мақсатты функция қауіптерді іске асырудан келтірілген залалды ғана емес, сонымен қатар, басқа шамаларды да білдіре алады. Мысалы, қосымша мыналарды ескеруге болады: ақпараттандыру объектісіндегі ақпараттық ресурстардың жалпы шығындары; ақпараттандыру объектісіндегі ақпаратты қорғау құралдарына инвестициялаудан түскен пайда, инвестициялардың рентабельділігі және т. б. (2.7) функциясы үшін оңтайлылық критерийін қолдану нұсқалары генетикалық алгоритм қолдану тұрғысынан мүмкін. Қосымша шарттар енгізілуі мүмкін, атап айтқанда, қорғаныс жағының ресурстарының мөлшеріне немесе $o(h,d)$ бойынша. $v(h,d)$ тәуелділіктерді анықтау кезінде келесі ойлар ескерілді. Сәтті шабуылдың ықтималдығы шабуылды жүзеге асыру h шығындарына тікелей пропорционалды және объектіні қорғауға жұмсалатын d шығыстарға кері пропорционалды. Сондықтан *v(h,d)*-ға кіретін *h,d* айнымалылары $r=h/d$. қатынасы ретінде енеді. Жазбаны азайту үшін кейбір жағдайларда біз $d=const$ деп аламыз және *v(h)* тәуелділігін *h* салыстырмалы шама деп қарастырамыз. *v(h,d)*- тәуелділіктері келесі шарттарды қанағаттандыруы керек:

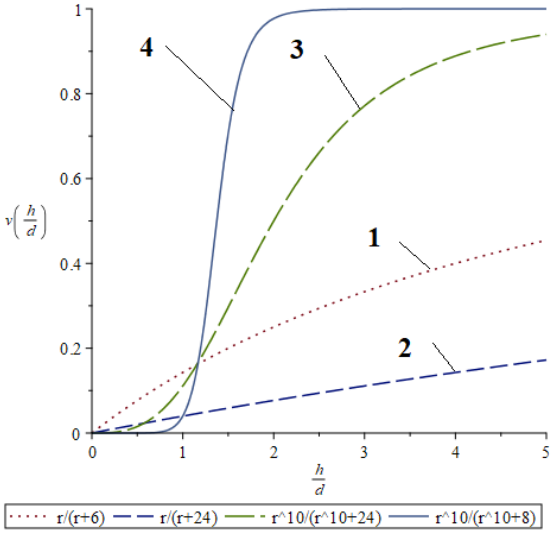
$$r=\left(h/d\right)\to 0, \quad v(h,d)\to 0 \quad \text{және} \quad r=\left(h/d\right)\to\infty,\ v(h,d)\to\infty .$$

Сәйкесінше, біз $y=\left(d/h\right)$ қабылдаймыз. Бұл шарттар түрдің дәрежелік пен көрнекі функцияларын қанағаттандырады [64, 120-б.]:

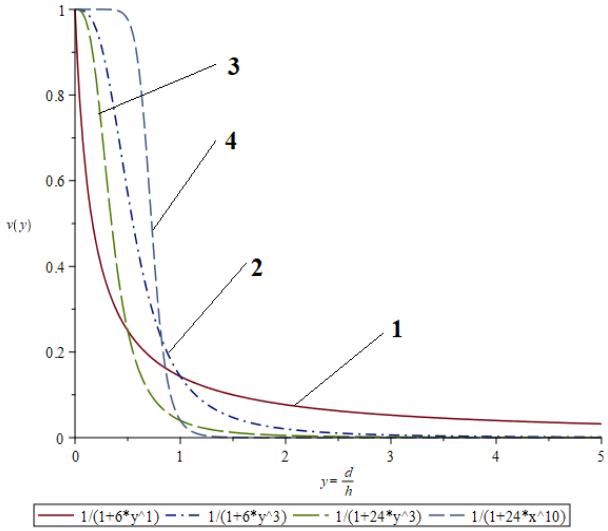
$$v(h,d)=r^n/\left(r^n+a\right) \tag{2.8}$$

$$v(h,d)=1-e^{-b\cdot r^n}, \tag{2.9}$$

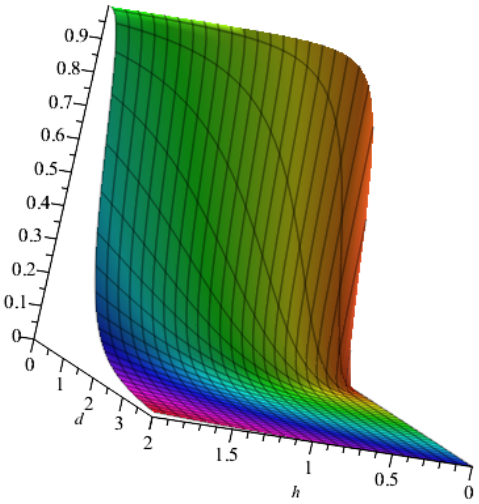
Мұндағы *a,b,n* - 2.2–2.5-суреттерінде көрсетілген қисықтардың орны мен формасын анықтайтын тұрақтылар.



2.2-сурет. Түрдің дәрежелік функциясы үшін тәуелділіктер (2.8)

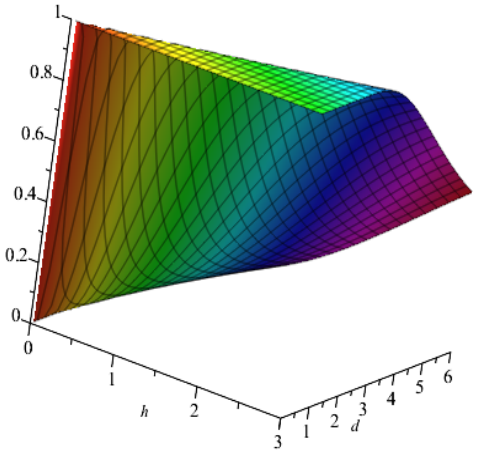


2.3-сурет. Түрдің көрнекі функциясы үшін тәуелділіктер (2.9)



r^3)/(r^3+8)

2.4-сурет. Түрдің дәрежелік функциясының бетіне тәуелділіктер (2.8)



1-exp(-3(r)^2

2.5-сурет. Түрдің көрнекі функциясының бетіне тәуелділік (2.9)

Шешілетін есеп тұрғысынан ақпараттандыру объектісі үшін ақпаратты қорғау құралдары шығындарының *a,n* өнімділігі немесе жалпы жағдайда нақты ақпаратты қорғау құралдары тиімділігінің

көрсеткіштері мен оларды сатып алу, қызмет көрсету, жаңғырту шығындарының көрсеткіштері. Екі тәуелділіктің де формасы ұқсас екенін ескере отырып, олар жоғарыда аталған жағдайларды қанағаттандыратындықтан, болашақта қорғаныс ресурстарын адаптивті бөлу есебін шешудің генетикалық алгоритмін орындау кезінде қарапайым бөлшек-дәрежелік функциялары қолданылды (2.8). $n=1$ -де бұл бөлшек-сызықтық тәуелділікті білдіреді. Егер $n>1$ болса функция бөлшек-сызықты емес.

$n=1$-де осалдықтардың бөлшек-сызықтық функциялары ақпаратты қорғау құралдарына жауап береді, олар үшін $\left(h/d<1\right)$ бастапқы кезеңдерде де инвестиция салу нәтиже береді. Мысалы, периметрді қорғауға, жалған электромагниттік сәулелену және кедергілер (ПЭМИН) арналары арқылы тарап кетуден қорғауға және т.б. байланысты шараларды енгізу ақпараттандыру объектісі қауіпсіздігінің жалпы дәрежесіне оң әсер етеді. Бөлшек-сызықты емес $n>1$ болса функциялар күрделі техникалық ақпаратты қорғау құралдарының осалдығын сипаттайды. Мысалы, криптографиялық жүйелер. Кілт жоғалған (немесе бұзылған) немесе криптографиялық алгоритмнің осалдығы анықталған сәтке дейін инвестициялар салу нәтиже бермейді, осы сәттен кейін криптожүйенің осалдығы күрт артады. Сол сияқты, вирусқа қарсы қорғаныста және вирусқа қарсы бағдарламалық қамтамасыз ету базаларын жүйесіз жаңарту да жүйенің осалдығының өсуіне әкелуі мүмкін. n шамасы неғұрлым үлкен болса, кедергі шабуылдарға осал емес шекті мән соғұрлым үлкен болады. Сонымен қатар, қорғаныс жағы мен шабуылдаушылар ресурстарының арақатынасы шекті мәннен асқан кезде өсу аймағы соғұрлым тез артады.

Коэффициентті ақпараттандыру объектісіндегі табиғи қауіпсіздік ретінде түсіндіруге болады. Мысалы, типтік ұсыныс - басқа бөлмелермен іргелес есіктері жоқ және баспалдақтар мен шығу есіктерінен алыс орналасқан жеке бөлмелердегі шағын желілердің серверлік бөлмелерін жабдықтау. Сондай-ақ, серверлік бөлмелерге қол жеткізе алатын адамдар тобын шектеу ұсынылады және т.б. Дегенмен, бұл ұсыныстарды бәрі бірдей орындай бермейтінін мойындау керек. (2.8) және (2.9) мақсат функцияларды қабылдай алатын шектер мен рұқсат етілген мәндерді анықтау үшін шоғырландырылған ақпаратты жинау және талдау талап етіледі. Мұндай

ақпараттың көзі - ақпараттық қауіпсіздік және киберқауіпсіздік салаларына қатысты есептер. Мысалы, компанияның көлеміне байланысты ақпаратты қорғауға ақпараттық технологиялар бюджетінің 1%-дан 30%-на дейін кетеді, ал ақпараттың жоғалуы 0-дан 4%-ға дейінгі диапазонда қолайлы деп саналады, бұған қосымша 20%-дан астам ақпараттық активтердің жоғалуы 60%-ға дейін компанияның құлдырауына және банкроттыққа әкеледі [10. 188-б.]. Негізгі есеп қорғаныс тұрғысынан шешім табу болғандықтан, осалдық функциясын (2.8) келесідей ұсынуға болады:

$$v(y) = 1 \Big/ \left(a \cdot y^n + 1\right) \qquad (2.10)$$

мұндағы $y = d \Big/ h$

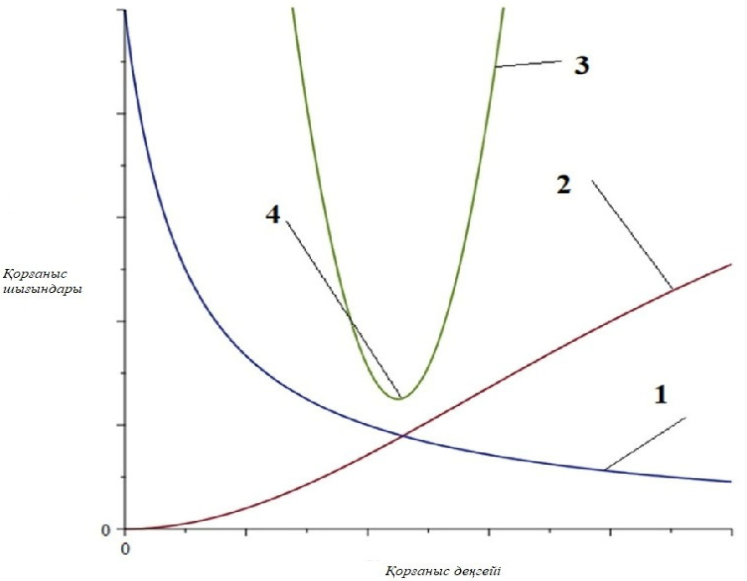
Тәуелділікті модельдеу нәтижесінде (2.8) және (2.10) сәйкесінше 2.2, 2.4 және 2.3,2.5-суреттерде көрсетілген. $r \to \infty$ -де алынған графиктерден n және a көрсеткіштер бойынша көрінеді және қисықтың пішініне әлсіз әсер етеді. Бұл қисық n және a кез келген түрде болса да бірлікке асимптотикалық жақындайтындығымен байланысты. $0 < r < 1$ -де n шамасы, негізінен, дөңес пішінге, ал a - абсцисса осінен жоғары қисықтың көтерілу биіктігіне әсер етеді.

n және a параметрлердің тәуелділік формасына әсері (2.10) 2.3, 2.5- суреттерінде көрсетілген. n параметрдің әсері негізінен $d < 1$ бастапқы аймақта көрінеді. $n \le 1$ -де қисықтардың дөңестігі төмен, $n > 1$ -де жоғары бағытталған. a параметр абсцисса осінен жоғары қисықтардың көтерілу биіктігіне әсер етеді. a шаманың өсуімен осалдық азаяды және қисықтар төменге түседі. Бөлшексызықтық функциялар ақпаратты қорғау құралдарына ($d \approx 0$) бастапқы инвестициялар (ұйымдастырушылық, инженерлік-техникалық іс-шаралар мен техникалық ақпаратты қорғау құралдарына) осалдықты монотонды төмендетуге және нұқсанның азаюына әкелетін материалдық жеткізгіштерде сақталатын ақпараттың осалдығын сипаттайды. Әрі қарай d ұлғайған сайын, ақпаратты қорғау құралдарына акша салу тиімділігі төмендейді (бұл пайданың шекті нормасы туралы экономикалық заңға байланысты).

Бөлшек-сызықты емес ($n > 1$, 3, 4-қисықтар, 2.2-сурет) функциялар кедергіні еңсеру үшін айтарлықтай ресурстарды жұмсау қажет болатын компьютерлік жүйелерде айналымдағы ақпараттың қасиеттерін көрсетеді. n көрсеткішінің (2.8) артуы есебінен сызықтық емес өсу кезінде $v(h,d)$-қисық нысан бойынша сатыға жақындайды. Жүйені бұзу үшін айтарлықтай ресурстар қажет болған кезде, мұндай тәуелділік деректерді шифрлауды қолдану кезінде байқалады, содан кейін ақпараттық қауіптерді іске асырудан келтірілген залал күрт артады. $0 < n < 1$ кезінде (2.8) функция ақпараттың абайсызда болған қауіп-қатердің әсеріне бейімділігін сипаттайды. Кездейсоқ қауіптерге, мысалы, персоналдың қабілетсіздігі, жабдықтың істен шығуы және т.б. мұндай жағдайларда ақпараттық ресурс иесіне шабуылдаушылар ресурстарды жұмсамай зиян келтірілген. Әр жүйе үшін a,b,n параметрлерді таңдау маңызды есеп болып табылады. a,b,n параметрлердің шамасына техникалық, технологиялық, ұйымдастырушылық, құқықтық, моральдық-этикалық және физикалық ақпараттық қауіпсіздік шаралары әсер етеді. Осы шаралардың бір бөлігінің әсері монографияның келесі тармағында және келесі тарауларында егжей-тегжейлі қарастырылады. Сәтті шабуыл ықтималдығының шабуыл мен қорғаныс ресурстарының арақатынасына тәуелділік формасын белгілеу есепі өте күрделі және әр нақты жүйе үшін бөлек шешіледі. Тәуелділіктің айқын түрі (2.8) сараптамалық бағалау негізінде немесе статистикалық деректер негізінде белгіленеді.

Ақпаратты қорғау құралдары құру және ақпараттық қауіпсіздік стратегиясы мен саясатын жоспарлау кезінде нақты ақпаратты қорғау құралдары ерекшеліктерін ескере отырып, мақсатты функцияны оңтайландыруды орындау маңызды. Қорғау тарапының ресурстарын жобалау немесе бөлу сатысында бастапқы параметрлерді бағалау кезіндегі қате ақпараттық активтердің айтарлықтай жоғалуына әкеледі. $v(h,d)$-алынған мәндер минималды нәтижеге кепілдік бере алмайтындығын ескереміз, өйткені рұқсат етілген мәндердің шекарасы ершік нүктенің болуымен және берілген тепе-теңдік нүктесінен солға немесе оңға ауытқуымен анықталады, 2.1, 2.2 және 2.5-суреттерді қараңыз. Мұндай ауытқу шексіз циклдік процеске әкеледі, онда ешқандай қорғаныс стратегиясы тұрақты нәтижеге кепілдік бермейді. Сондай-ақ, a параметрі мақсатты функцияның оңтайлы әсеріне айтарлықтай әсер ететін-

дігін ескеру қажет. Атап айтқанда, АР-ны объектілер бойынша ұтымды бөлу, неғұрлым қорғалған объектілерде АР-дің көп мөлшері болған кезде, D қорғауға арналған ресурстардың бірдей мөлшерімен тиімділігі зор.



2.5-сурет. Ақпаратты қорғауға ресурстарды бөлуді оңтайландырудың жалпы схемасы

1 - шабуылдардан және ақпараттық ресурс жоғалудан күтілетін шығындар;

2 - ақпаратты қорғау құралдарына арналған шығындар;

3 - күтілетін жиынтық шығындар;

4 - оңтайлы мән

Ақпаратты қорғау құралдары құру кезеңінде оңтайлы шешімді іздегенде қарсыластың кез келген іс-әрекеті кезінде біраз уақытқа кепілдендірілген нәтижені қамтамасыз ететін ершік нүктесінің (4) режимі тек белгілі бір құрылымдар үшін және шабуылдаушы тараппен қарсыласудың белгілі бір жағдайларында ғана бар екенін ескеру қажет. Бұл режимді қамтамасыз ету объектілердің осалдығын анықтайтын параметр мәндерін таңдау арқылы жүзеге

асырылады. Ресурстардың қажетті санын және оларды объектілер арасында бөлуді айқындайтын (2.8) және (2.9) мақсат функциялар беттеріндегі жұмыс нүктесін таңдау критерийі мынадай көрсеткіштерді қамтамасыз ету болып табылады, 2.3. және 2.4-суреттерді қараңыз: бір жақты қарама-қайшылық үшін - ақпараттық ресурс шығындары мен оны қорғауға арналған шығындарды біріктіретін жалпы шығындардың минимумы, екі жақты жағдайда – жалпы пайданың максимумы (ақпаратты қорғау құралдарына инвестициялар салудан түсетін пайданың сомасы және қорғаушы тарап үшін шабуылдаушы тарап туралы ақпарат алудан түсетін пайда немесе симметриялы – ақпараттандыру объектісіне шабуыл жасау құралдарына инвестициялар салудан түсетін пайданың және қорғаныс тарабы үшін шабуыл жасаушы тарап туралы ақпарат алудан түсетін пайда туралы ақпарат). Оңтайлы стратегияны іске асырудың сенімділігіне қосымша талаптарды сақтау арқылы қол жеткізіледі: жұмыс нүктесі көрсетілген шарттар орындалатын аралықтың шекарасынан біршама қашықтықта болуы, сонымен қатар жұмыс нүктесінің маңында объектілердегі ресурстардың оңтайлы арақатынасында айтарлықтай өзгерістер болмауы керек. Осы жағдайларды қамтамасыз ету қажетті ресурстарды анықтауға мүмкіндік береді, сайып келгенде, ақпаратты қорғау құралдары, бұл ақпараттандыру объектісі үшін оңтайлы ақпаратты қорғау құралдарын құруға жол ашады.

2.2. Кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді оңтайландыру есепін шешуге арналған генетикалық алгоритм

Монографияның бірінші тарауында жүргізілген талдау нәтижесінде генетикалық алгоритмдердің ресурс мөлшеріне қойылған таңдау мен шектеулердің көп критерийлілігі жағдайында ресурстарды бөлуді оңтайландыру есептеріндегі бірқатар маңызды артықшылықтары анықталды. Біріншіден, генетикалық алгоритм дәстүрлі әдістердегідей іздеу кеңістігін нүктеден нүктеге бірізді қарастырудың орнына, бір уақытта бірнеше шешім нұсқасын қатар қарастырады. Бұл тәсіл классикалық оңтайландыру әдістеріне тән кемшіліктердің бірі болып саналатын мақсатты функцияның

жергілікті экстремумына түсіп қалу қаупін айтарлықтай азайтады. Нәтижесінде жаһандық оңтайлы шешімге қол жеткізу ықтималдығы жоғарылайды. Екіншіден, генетикалық алгоритм жұмыс барысында қосымша көмекші ақпаратты талап етпейді. Яғни, есепті шешу кезінде тек қана мақсатты функцияның мәндері және іздеу кеңістігінің параметрлері пайдаланылады. Бұл ерекшелік алгоритмнің есептеу жылдамдығын арттырып, күрделі есептерді шешуде уақыттық тиімділікті қамтамасыз етеді. Ерекше жағдай ретінде тек еркін нүктеде параметрлердің және мақсатты функцияның рұқсат етілген мәндерінің жиынтығын есепке алу қажеттілігі атап өтіледі. Үшіншіден, генетикалық алгоритм жаңа шешімдерді қалыптастыруда ықтималды ережелерді (мутация, кроссовер) қолданумен қатар, бір шешімнен екіншісіне өту кезінде детерминделген ережелерді де пайдаланады. Мұндай тәсіл кездейсоқтық пен детерминизм элементтерінің үйлесімділігін қамтамасыз етіп, олардың жеке-жеке қолданылуына қарағанда әлдеқайда тиімді нәтижеге қол жеткізуге мүмкіндік береді. Төртіншіден, генетикалық алгоритмдердің тағы бір маңызды артықшылығы – олардың бейімделгіштігі. Іздеу процесінде аралық шешімдердің сапасына байланысты популяция құрамын үздіксіз өзгерту мүмкіндігі бар. Бұл өзгермелі және белгісіз орта жағдайларында да тиімді шешім табуға жағдай жасайды. Соңында, генетикалық алгоритмдер көп критерийлі есептерді шешуде әмбебап құрал болып табылады. Олар бір уақытта бірнеше мақсатты функцияны оңтайландыруға мүмкіндік береді, ал бұл өз кезегінде ресурстарды бөлудің күрделі жағдайларында неғұрлым ұтымды нәтижелерге қол жеткізуге жол ашады Осылайша, генетикалық алгоритмдердің аталған артықшылықтары оларды киберқауіпсіздік, ақпаратты қорғау және ресурстарды басқару сияқты күрделі жүйелердегі шешім қабылдау міндеттерінде қолданудың тиімділігін дәлелдейді. Жоғарыда айтылғандарды ескере отырып, монографиялық жұмыстың осы бөлімінде ақпаратты қорғау құралдары шығындарының экономикалық орындылығының көрсеткіштерін анықтау және объектілер арасында қорғаныс жағының ресурстарын адаптивті қайта бөлу қажет болған жағдайда оңтайлы шешімді іздеу үшін генетикалық алгоритм синтезі есепсі шешіледі.

Генетикалық алгоритмнің жұмыс принципі табиғи эволюция мен популяциялық генетика механизмдерін модельдеуге негіз-

делген [76]. Графикалық түрде генетикалық алгоритм жұмысының схемасы 2.6-суретте көрсетілген.

Монографиялық жұмыстың осы бөліміндегі *a,n* параметрлерді анықтау үшін генетикалық алгоритмді ақпараттандыру объектісі кибернетикалық қауіпсіздігін қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді оңтайландыру есепін шешу үшін пайдалану ұсынылады. Ресурстарды бөлу көбінесе бұрын көрсетілгендей ақпараттық ресурстардың осалдығының мақсат функциясының түріне әсер ететін *a,b,n,* шамаларды айқындайды (2.10). Генетикалық алгоритм келесі терминологиямен жұмыс істейді [70, 16-б.]:

Хромосома – тұқым қуалайтын ақпараттың тасымалдаушысы. Хромосомалардың жиынтығы (әр хромосома үшін мақсатты функцияның немесе мақсат функция параметрінің мәні бар) жеке дарақты сипаттайды. Хромосома гендерден тұрады.

Гендер – тұқым қуалайтын ақпаратты кодтау элементтері. Ақпаратты биттік кодтау гендер ретінде пайдаланылуы мүмкін (яғни, биттердің көмегімен мақсат функцияны сипаттауға болады).

Дарақ(Особь) – хромосомалардың жинағы. Дарақ – бұл генетикалық алгоритм қолдану кезінде мақсат функция мәнін іздейтін параметрлер жиынтығы.

Дарақтың жарамдылығы – бұл мақсат функцияның қажетті мәніне қатысты осы параметрлер жиынтығы үшін мақсат функция мәні.

Генетикалық алгоритм әрекеті [70, 22-б.]: Хромосомалардың бастапқы популяциясының генерациясы – кездейсоқ таңдалған мақсат функция мәндері.

Селекция – көбею үшін ең жақсы бейімділігі бар дарақтарды таңдау. Таңдауды мақсат функция мәні бойынша сұрыптау деп түсіндіруге болады. Жеке дарақтардың бейімделу мәні неғұрлым жоғары болса, олардың ата-аналық гендердің келесі ұрпақтарында шағылыстыру және мұрагерлік мүмкіндігі соғұрлым жоғары болады.

Кроссовер (немесе кроссинговер) - шағылыстыру. Кездейсоқ түрде ата-аналардың хромосомаларының биттері арасындағы үзілу нүктесі таңдалады. Үзілу нүктелері – жолдағы іргелес биттер арасындағы бөліктер. Ата-аналық құрылымдар белгілі бір уақытта екі сегментке бөлінеді. Әртүрлі ата-аналар дарақтарының тиісті

сегменттері бір-біріне жапсырылады. Жапсырылғаннан кейін ұрпақтардың екі генотипі алынады.

2.6-сурет. Генетикалық алгоритм жұмысының жалпы сызбасы

Жоғарыда айтылғандай, ақпараттандыру объектісі үшін ақпаратты қорғау құралдары шығындарының өнімділігін сипаттайтын *a,n* параметрлер функционалды *v(h,d)*-тәуелділіктің түріне айтарлықтай әсер етеді.

2.1-кестеде ақпараттандыру объектісі үшін ақпараттық ресурс осалдық дәрежесіне әсер ететін *a* параметрін зерттеу мысалында көрсетілген есепті шешудің бастапқы деректері көрсетілген.

2.1-кесте – Есепті шешудің бастапқы параметрлері

Ақпараттандыру объектісінде *ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстардың тізбесі (а –ның ең жоғары мәнін айқындау үшін)*		
№	Жұмыстар тізімі	Белгіленуі
1	Кешенді ақпаратты қорғау құралдары жобалау, әзірлеу және орналастыру	***A***
2	Ақпараттық қауіпсіздік қамтамасыз ету жүйесін жетілдіру	***B***
3	Ақпараттық қауіпсіздік қақтығыстарын анықтау, қақтығыстарға ден қою, ақпараттандыру объектісі үшін тәуекелдерді болжау	***C***
4	Ақпараттық қауіпсіздік жеке объектілері арасындағы байланыстарды азайту және қысқы қаттылық компонентерін біріктіру	***D***
5	Ақпараттандыру объектісі бизнес процестерінің ерекшелігіне сәйкес келетін ақпараттық қауіпсіздікті ұйымдастыру шараларын әзірлеу	***E***
Бөлінетін ресурстарды шығыстар баптары бойынша топтастыру (Ресурстарды ақпараттық қауіпсіздік және киберқауіпсіздік инвестициялау түрлері)		
1	Ақпараттық қауіпсіздікке арналған материалдық және қаржылық шығындар	МҚШ
2	Ақпараттық қауіпсіздік және ақпараттандыру объектісі киберқауіпсіздік қамтамасыз ету бойынша жобаларға тартылған адам ресурстары	АР
3	Ақпараттық қауіпсіздік және ақпараттандыру объектісі киберқауіпсіздік саласындағы жобаларды басқаруға арналған шығындар	БШ
4	Ақпараттық қауіпсіздік және ақпараттандыру объектісі киберқауіпсіздік қамтамасыз етуге арналған басқа да шығындар	ӨШ
АҚО үшін ақпараттық қауіпсіздік және киберқауіпсіздік бойынша іс-шараларды енгізуден бәсекелестік артықшылықтар		
1	Бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар	БҚ
2	Инновацияларды дамыту және бизнес процестерге цифрлық технологияларды енгізу	ИД
3	Ақпараттық технология шығындарын азайту	ША

a,n параметрлерді анықтау процесінде ұтымдылық критерийлерін келесідей сипаттауға болады:

$$F_k = \sum_i \sum_j I_j \cdot E_{ijk} \cdot X_{ijk} \xrightarrow{\sim} \max, \qquad (2.11)$$

мұнда $k = 1,2,3$ 2.1-кестеде оптималдылық критерийлері үшін ($k = 1$ (бағдарламалық қамтамасыз ету үшін), $k = 2$ (ИД), $k = 3$ (ША);

I_j – киберқауіпсіздік және ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлудің таңдап алынған оңтайлы нұсқасындағы басымдық (маңыздылық) (2.1-кестені қараңыз.), $\sum I_j = 1$;

$i = 1(A),2(B),3(C),4(D),5(E)$ – жұмыс түрлері жұмыс тізбесінен көрініс (1-кестені қараңыз, ақпараттандыру объектісі ерекшеліктеріне байланысты өзгеруі мүмкін);

$j = 1$ МҚШ үшін, $j = 2$ ақпараттық ресурс үшін, $j = 3$ БШ үшін, $j = 4$ ӨШ үшін (2.1-кесте) – ақпараттандыру объектісіне ақпараттық қауіпсіздік мен киберқауіпсіздікті қамтамасыз ететін қаражат пен шараларға инвестициялық салымдардың (ресурстардың) түрлері;

Ақпараттандыру объектісіне ақпараттық қауіпсіздік пен киберқауіпсіздікті қамтамасыз ететін қаражат пен шараларға инвестициялық салымдардың (ресурстардың) түрлері;

X_{ijk} – айнымалы, егер 2.1-кестедегі тізбедегі *i* жұмыс *j* инвестициялық салымды іске асыру үшін пайдаланылса, 1-ге тең. Болмаса, 0-ді қабылдаймыз;

E_{ijk} – *k* оңтайлылық критерийты қамтамасыз ететін *j* инвестициялық салымды іске асыру үшін орындалатын 2.1-кестедегі тізбедегі *i* жұмыс түрлерінің тиімділігі ;

$\xrightarrow{\sim}$ – *a,n* параметрлердің оңтайлы мәніне қол жеткізу.

Ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы жобаларды іске асыруға компанияда (кәсіпорында) бар бөлінетін ресурстарға шектеулерді былайша беруге болады:

$$Q = \sum_i \sum_j I_j \cdot l_{ijk} \cdot X_{ijk} \le A_j, \qquad (2.12)$$

мұнда l_{ijk} – k оңтайлылық критерийты қамтамасыз ететін i түріндегі жұмыстарды орындаумен байланысты j ресурстардың шығындары (немесе еңбек сыйымдылығы); A_j – k оңтайлылық критерийты қамтамасыз ететін i түріндегі жұмыстарды орындаумен байланысты j ресурстарды инвестициялау бойынша шектеу .

Есепті шешудің құрылымын анықтайтын шектеулер (немесе шешім матрицаларындағы 0 және 1 мәндерін қою) төменде сипатталған.

Шектеу (2.13) k -оңтайлылық критерийі үшін ақпараттандыру объектісінде ақпараттық қауіпсіздік пен киберқауіпсіздікті қамтамасыз ететін j ресурстар бағыты бойынша 2.1-кестедегі тізбеге сәйкес i жұмыстардың ең болмағанда біреуі пайдаланылатынын білдіреді:

$$\sum_i X_{ijk} \geq 1. \qquad (2.13)$$

Шектеу (2.14) k оңтайлылық критерийі үшін i түрдің жұмысы кезінде j ресурстар кем дегенде бір рет пайдаланылатынын білдіреді:

$$\sum_j X_{ijk} \geq 1. \qquad (2.14)$$

Шектеу (2.15) j ресурстарды бөлудің кез келген бағыты бойынша i түріндегі жұмыстардың кез келген бағытта k оңтайлылықтың ең болмағанда бір критерийін қалыптастыруға қатысуы тиіс дегенді білдіреді:

$$\sum_k X_{ijk} \geq 1. \qquad (2.15)$$

Есептің осы тұжырымында оңтайлы шешім табу проблемалары келесідей:

1) есеп көп критерийлі;

2) (2.13)–(2.15) шектеулердің түріне байланысты оңтайлы шешімдерді іздеудің белгілі әдістері тиімсіз болады немесе көптеген есептеу ресурстарын қажет етеді. Мысалы, қорғаныс объектілері үшін ақпараттық қауіпсіздік және киберқауіпсіздік құралдарының оңтайлы құрамын іздеу есептерінде кеңінен қолданылатын бұтақтар мен шекаралар әдісі [71] (дискретті бағдарламалаудың комбинаторлық әдісі) үкімді ішкі жиындарға (тармақтау деп аталатын) рұқсат етілген шешімдер жиынтығын

дәйекті түрде бөлуге дейін азайтады. Ішкі жиындар үшін сәйкесінше бағалар (шекаралар) есептеледі. Бұл, сайып келгенде, есептің шешімін анық қамтымайтын ішкі жиындарды жоюға мүмкіндік береді. Алайда, (2.13) - (2.15) шектеулерде теңсіздік белгілері бар. Сондықтан тармақталу ережелерін нақтылау және ішкі жиындардың шекараларын есептеу қиын немесе мүмкін емес. Мұндай пайымдауды осы көп критерийлі есепті шешудің басқа әдістеріне сәйкес келтіруге болады. Жоғарыда айтылғандарды ескере отырып, есептің шешімін іздеу алгоритмі ретінде (2.11)-(2.15) генетикалық алгоритмді қолдану ұсынылды, 2.7-суретті қараңыз.

Беллман–Заде принципіне негізделген шешімнің тартымдылығын есептей отырып, генетикалық алгоритм жалпыланған схемасы 2.7-суретте көрсетілген.

Жұмыстың басымдылығы сараптамалық жолмен, мысалы, ақпараттандыру объектісі ақпараттық қауіпсіздік жағдайының аудиті негізінде көрсетілуі мүмкін. Немесе алгоритмнің жұмыс қабілеттілігін тексеру үшін. Мысалы, 2.2-кестедегідей.

Ресурстарды ақпараттық қауіпсіздік және киберқауіпсіздік инвестициялау түрлер	Басымдық (B(2) үшін ақпараттық қауіпсіздікті қамтамасыз ету жүйесін жетілдіру)
Ақпараттық қауіпсіздікке арналған материалдық және қаржылық шығындар (МҚШ)	0,29
Ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік (РА) қамтамасыз ету жөніндегі жобаларға тартылған адами ресурстар	0,28
Ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік (БШ) саласындағы жобаларды басқаруға арналған шығындар	0,23
Ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік (ӨШ) қамтамасыз етуге арналған басқа да шығындар	0,2

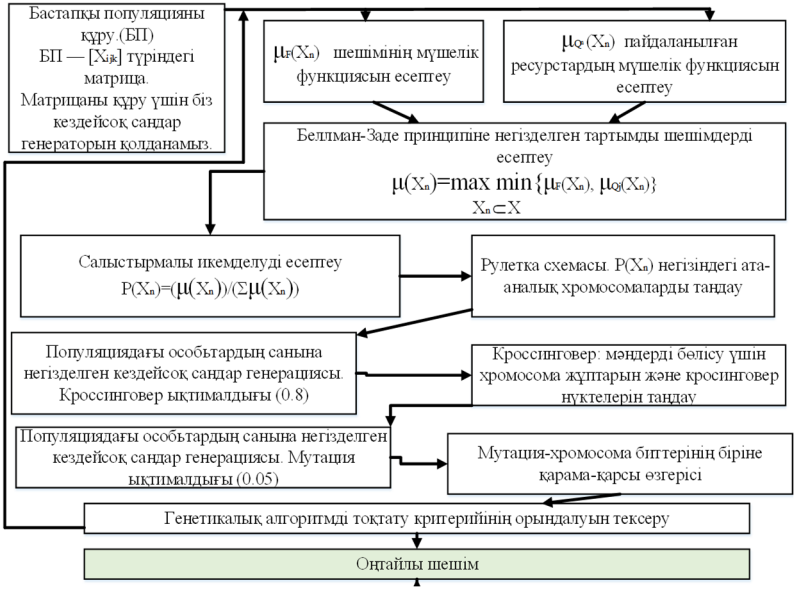
2.2-кесте – ақпараттандыру объектісінде жұмыстар жүргізудің басымдылығын бөлу мысалы

Біздің есепіміз үшін, жалпы жағдайда, модель түрдің үш $X^*_{ij1}, X^*_{ij2}, X^*_{ij3}$ оңтайлы шешімін табуды қамтиды (оңтайлылық критерийтардың санына сәйкес):

$$\left\| X^*_{ijk} \right\| = \begin{bmatrix} x^*_{11k} & x^*_{12k} \dots x^*_{1jk} \\ x^*_{21k} & x^*_{22k} \dots x^*_{2jk} \\ \dots & \dots \quad \dots \quad \dots \\ x^*_{i1k} & x^*_{i2k} \dots x^*_{ijk} \end{bmatrix}, \qquad (2.16)$$

Мұнда k оңтайлылық критерийінің нөмірі; $x^*_{ijk} = 0 \vee 1 -$ дарақ генінің мүмкін күйі.

Ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздікті қамтамасыз ету саласында қалыптасқан нақты тәсілдерді ескере отырып, кәсіпорын немесе компания 2.1-кестеде келтірілген барлық критерийтарды ескере отырып, бір уақытта тек бір ғана жұмыс түрін жүргізе алады деп қабылдаймыз. Бұл барлық жұмыстарды дереу жүргізу барлық қорғаныс объектілері үшін ақпаратты қорғау контурларының жұмысын бірден бұзатындығымен түсіндіріледі, сондықтан қысқа уақытқа болса да, барлық қорғауды әлсіретеді немесе жояды.



2.7-сурет. Беллман–Заде принципіне негізделген шешімнің тартымдылығын есептей отырып, генетикалық алгоритмнің жалпыланған схемасы

Сондықтан біз тек $i \in [1;5],\ j \in [1;4]$. екі индекс қатысатын X_{ij}^{*} оңтайлы шешімді табу есебін шешуге көшеміз.

Әр шешім түрдің екілік матрицасын білдіреді:

$$\|X_n\| = \begin{bmatrix} x_{11}\ x_{12}\ x_{13}\ x_{14} \\ x_{21}\ x_{22}\ x_{23}\ x_{24} \\ x_{31}\ x_{32}\ x_{33}\ x_{34} \\ x_{41}\ x_{42}\ x_{43}\ x_{44} \\ x_{51}\ x_{52}\ x_{53}\ x_{54} \end{bmatrix}, \qquad (2.17)$$

мұнда n дегеніміз Х - хромосоманың нөмірі және $x_{ij} = 0 \vee 1$. Генетикалық алгоритм қолдану үшін x_{ij} мәндерді екілік реттілік форматында кодтау керек. Шешімді немесе екілік матрицаны ұзындығы 20 биттік тізбектен тұратын хромосома ретінде елестетуге болады (5*4 өлшемді матрица).

Суретте мұндай жазбаны қабылдауды ыңғайлы ету үшін жеке топтарды 4 биттен бөлетін бос орындар қолданылады.

Бірінші популяция кездейсоқ сандар генераторының көмегімен жасалады. Бірінші кезеңде алты хромосома қаралды, 2.8-суретті қараңыз. 2.8-суретте көрсетілген әр реттілік генетикалық алгоритм үшін бастапқы популяцияны құрайтын алты хромосоманың бірі болады.

X_1=	1011	0011	1101	0001	1011
X_2=	0100	0110	1101	0101	0000
X_3=	1000	0000	1010	1101	0000
X_4=	0111	0011	0111	0001	1010
X_5=	0101	1010	0010	0110	1001
X_6=	1111	0011	1000	0101	1011

2.8-сурет. Генетикалық алгоритм үшін бастапқы популяция схемасы

Генетикалық алгоритм іске асыру барысында қолайлы шешімдерді таңдауда оңтайландыру есепін қою үшін әрбір мұндай шешімнің жарамдылығын бағалау қажет. Бөлінген ресурстарға шектеулер, сондай-ақ, оңтайлы нәтижелерге қол жеткізу анық емес деп санаймыз. Компаниялардың ресурстарды оңтайландыру іс-тәжірибесінде қорғаныс жағы – бұл жағдай [72] жұмыста егжей-тегжейлі сипатталған. Яғни, біз анық емес математикалық бағдарламалау есепсімен айналысамыз. Жоғарыда айтылғандардың негізінде Беллман-Заде принципін қолдана отырып, шешімнің тартымдылығын анықтау ұсынылады [73]. Математикалық тұрғыдан, бұрын қабылданған белгілерді ескере отырып, бұл принципті келесідей жазуға болады:

$$\mu(X_n) = \max_{X_n \subset X} \min\left\{\mu_F(X_n), \mu_Q^j(X_n)\right\} \tag{2.18}$$

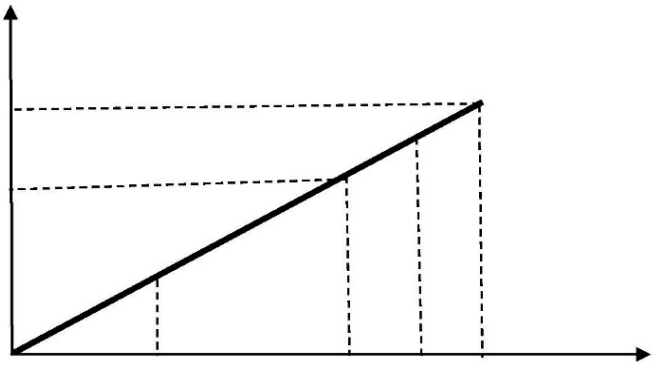
Модельдеу барысында алынған шешімдерді немесе яғни F_k критерийінің экстремалды мәнге жету дәрежесін бағалауға болады:

$$\mu(X_n) = \begin{cases} 0, \; for \; F(X_n) \le z - g; \\ \mu(X_n, g) \; for \; z - g < F(X_n) < z; \\ 1 \; for \; F(X_n) \ge z, \end{cases} \tag{2.19}$$

Мұнда $x \in [g, z]$, $g, z -$ жиынның шекаралары, 2.9-суретті қараңыз.

$F_{\max}, F_{\min} -$ тиісінше, 2.1-кестеде оңтайлылықтың үш критерийі үшін мүмкін болатын ең жоғары және ең төменгі мәндер (*k=1* (бағдарламалық қамтамасыз ету үшін), *k=2* (ИД), *k=3* (ША). Генетикалық алгоритм көмегімен есептерді шешу барысы бойынша $F_{\max}, F_{\min}$ – мәндер қорғау тарабының ресурстары шектелмеген деген болжам негізінде айқындалады және ол тиісінше 2.1-кестеде қамтылған жобалар бойынша барлық жұмыстарды іске асыра алады. Қарама-қарсы жол беру - қорғау жағында жобаларды жүзеге асыру үшін ресурстар жоқ. Шабуылдаушы

тарап үшін, қажет болған жағдайда, алдыңғы бөлімде сипатталған теориялық және ойын модельдерінің аппаратын қолдана отырып, пайымдауды осылай жасауға болады.



2.9-сурет. Шешім сапасын анықтау процесінде тиістілік функциясын алудың жалпы схемасы

Барлық $F_{\min}$ мәні үш k –үшін де бастапқыда нөлге тең. $F_{\max}$ мәнін (2.11) формуланы қолдану арқылы табуға болады.

k оңтайлылық критерийты қамтамасыз ететін j инвестициялық салымды іске асыру үшін орындалатын 2.1-кестедегі тізімдегі i жұмыс түрінің тиімділігі үшін E_{ijk} – мәндерді сараптамалық сауалнама негізінде анықтаймыз. X_{ijk} – бірлік матрицасы. Бұл жағдайда $x_{ijk} = 1$. Мысалы, деректерді өңдеу кезінде ресурстарды бөлу есебін шешу барысында келесі кесте алынды, 2.3-кестені қараңыз. Жұптық салыстырулардың матрицасы Т.Саатидің иерархиялық әдісін [74] және арнайы бағдарламалық қамтамасыз ету немесе Excel-де қолдану негізінде құрылады, 2.10-суретті қараңыз.

Кесте 2.3 - оңтайлылық критерийлері және ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік ресурстарына инвестициялау түрі үшін жұптық салыстыру матрицалары

k_1 оңтайлылық критерийі	$j=1$ МҚШ	$j=2$ АР	$j=3$ БШ	$j=4$ ӨШ
A	25	3	5	3
B	72	4	6	5
C	23	2	7	2
D	52	6	1	7
E	26	4	5	6
k_2 оңтайлылық критерийі	$j=1$ МҚШ	$j=2$ РА	$j=3$ БШ	$j=4$ ӨШ
A	45	6	7	7
B	32	2	5	1
C	55	2	1	2
D	71	6	3	3
E	25	4	4	3
k_3 оңтайлылық критерийі	$j=1$ МҚШ	$j=2$ РА	$j=3$ БШ	$j=4$ ӨШ
A	76	4	5	4
B	22	2	5	2
C	51	2	1	2
D	58	6	1	7
E	27	4	4	5

Есептеулер нәтижесінде біз мұндай мәндерді аламыз $F_{\max 1}=72{,}86$, $F_{\max 2}=79{,}56$, $F_{\max 3}=80{,}54$.

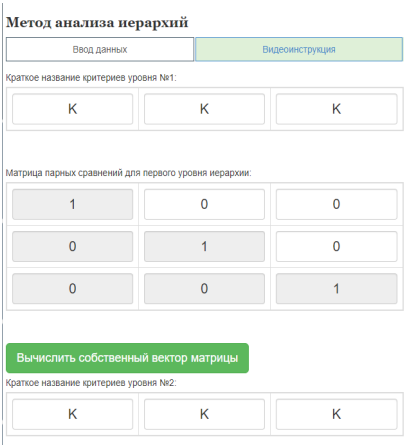
Осылайша, алынған шешімнің сапасына қатысты функцияны толық анықтауға болады – $\mu_F(X_n)$.

Әр шешімнің жарамдылығын өрнек негізінде бағалаймыз (2.8). Түр ресурстарына шектеуді орындау дәрежесі (2.2) жалпы жағдайда келесі тиістілік функциясымен сипатталады:

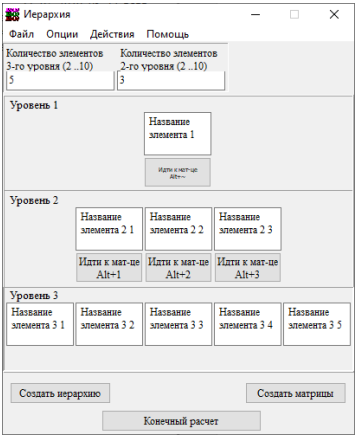
$$\mu_Q^j(X)=\begin{cases}0,\ for\ Q^j(X_n)\geq Q^{j*};\\ \left(Q^{j*}-Q^j(X_n)\right)/\left(Q^{j*}-A^j\right)\ for\ \ A^j<Q^j(X_n)<Q^{j*};\\ 1\ for\ Q^j(X_n)\geq A^j,\end{cases} \tag{2.20}$$

Q^{j*} – (2.20) өрнектің сол жақ бөлігі үшін барынша рұқсат етілген мәндер;

$Q^{j}(X_n)$ – (2.20) хромосома үшін есептелген өрнектегі сол жақ бөліктің мәні.



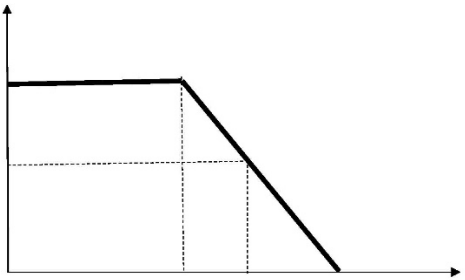
а) - Онлайн сервистің көмегімен Т. Саатидің иерархиялық әдісін қолдану негізінде жұптық салыстыру матрицаларын құру мысалы



б) - Сериялық бағдарламалық қамтамасыз ету қолдана отырып, Т. Саатидің иерархиялық әдісін қолдану негізінде жұптасқан салыстыру матрицаларын құру мысалы

2.10-сурет. Т. Саатидің иерархиялық әдісін қолдану негізінде жұптасқан салыстыру матрицаларын құру мысалдары

Графикалық түрде, өрнекке (2.19) сәйкес тиесілік функциясын осылай көрсетуге болады, 2.11-суретті қараңыз.



2.11-сурет. Ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздікті қамтамасыз ету үшін пайдаланылатын ресурстардың тиістілік функциясының жалпы схемасы

Бұрын көрсетілгендей, ақпараттық қауіпсіздік және киберқауіпсіздік бойынша жобаларға жұмсалған ресурстар мөлшеріне шектеу сараптамалық бағалауды қолдану нәтижесінде белгіленген.

Мысалы, жұмыстың осы параграфының шеңберінде өлшемсіз көріністе ресурстарға (ұлттық валюталарға байланыстырмай шартты ақша бірліктерінде) мұндай шектеулер қойылды. Бірінші ресурс үшін (ақпараттық қауіпсіздік – МҚШ-ға арналған материалдық және қаржылық шығындар, тиісінше $A^j = 40,\ Q^{j^*} = 50.$ Қалған ресурстар - РА, БШ, ӨШ үшін тиісінше $A^j = 2,\ Q^{j^*} = 3.$ $Q^j(X_n)$ функция мына формула бойынша есептеледі:

$$Q^j(X_n) = \sum l_{ijk} \cdot x_{ijk}, \qquad (2.21)$$

мұнда l_{ijk} – *k*-оңтайлылық критерийін қамтамасыз ететін *i*- түрдегі жұмыстарды орындаумен байланысты *j* ресурстардың шығындары (немесе еңбек сыйымдылығы).

A-E жұмыс түрлерінің ұсынылған жіктемесіне (2.1-кестені қараңыз) және ақпараттық қауіпсіздік бойынша әртүрлі жұмыс түрлері үшін техникалық-экономикалық көрсеткіштерді (ТЭК) анықтаудың қолданыстағы әдістемелеріне сәйкес есеп жүргізу үшін әр нақты жұмыс түрінің құны анықталады [76]. Содан кейін алынған мәндер өлшемсіз түрге келтіріледі, мысалы, негізгі шкаланы қолдана отырып [76]. Барлық субъективті көрсеткіштерді (мысалы, сарапшылардың біліктілігі мен жұмыс тәжірибесі) жұмыс құнының көрсеткіштерінде ескереміз.

Осылайша, оптималдылықтың тиісті өлшемін қамтамасыз ету үшін жұмыстың күрделілігі мен шығындарын ескеретін l_{ijk} түрін-дегі матрицаларды құруға болады. Нәтижелер 2.4-кестеде келті-рілген.

Жұптық салыстырудың матрицаларын құру үшін иерархияны талдау әдісі де қолданылды.

2.4-кесте – ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік ресурстарына инвестициялаудың оңтайлылық өлшемдері мен түрлеріне арналған жұмыстардың еңбек сыйымдылығының матрицалары

k_1 оңтайлылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	23,52	0,65	0,83	0,61
B	15,2	0,41	0,61	0,61
C	12,02	0,21	0,71	0,81
D	17,23	0,51	0,22	0,81
E	22,15	0,21	0,11	0,41
k_2 оңтайлылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	16,72	0,12	0,11	0,51
B	21,32	0,21	0,71	0,11
C	13,89	0,61	0,51	0,81
D	11,22	0,11	0,82	0,21
E	14,34	0,62	0,81	0,22
k_3 оңтайлылық критерийі	$j=1$	$j=2$	$j=3$	$j=4$
	МҚШ	АР	БШ	ӨШ
A	13,91	0,41	0,71	0,21
B	15,2	0,41	0,61	0,61
C	16,92	0,61	0,81	0,71
D	21,98	0,21	0,81	0,71
E	11,81	0,51	0,31	0,31

Барлық қажетті мәліметтермен популяцияның барлық хромосомалары үшін бейімделу функциясының мәндерін табуға болады (2.8-суретті қараңыз).

Егер хромосома шектеулерді (2.3)–(2.5) қанағаттандырмаса, онда оның фитнес функциясының мәні нөлге тең болады.

Зерттеудің келесі кезеңінде генетикалық алгоритмді іске асыратын бағдарламалық өнім сипатталатындықтан, параграф аясында жоғарыда келтірілген және 2.8-суретте көрсетілген алты хромосоманың бірінші $X_1 = 1011\ \ 0011\ \ 1101\ \ 0011\ \ 1011$ үшін шешімнің тартымдылығын есептеуді ғана егжей-тегжейлі қарастырамыз.

k критерийі үшін (ақпаратты және ақпараттық қауіпсіздік саясатын тиімді қорғау нәтижесі ретінде компания үшін бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар) $\mu_Q^j(X_1)$ тиістілік функциясын анықтаймыз. Ол үшін матрицаны 2.4-кестенің жоғарғы жағынан (k_1 критерийі үшін) $X_1 = 1011 \quad 0011 \quad 1101 \quad 0011 \quad 1011)$ хромосомаға көбейту керек. Содан кейін нәтижелерді бағандар бойынша қорытындылау керек. Нәтижесінде біз 2.5 түріндегі кестені аламыз.

2.5-кесте – ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік ресурстарына инвестициялаудың оңтайлылық критерийі және түрлері үшін хромосомаларды трансформациялау матрицалары

Бастапқы мәндер				
A	23,52	0,65	0,83	0,61
B	15,20	0,41	0,61	0,61
C	12,02	0,21	0,71	0,81
D	17,23	0,51	0,22	0,81
E	22,15	0,21	0,11	0,41
Есептеу нәтижелері				
A	23,52	0,00	0,83	0,61
B	0,00	0,00	0,61	0,61
C	12,02	0,21	0,00	0,81
D	0,00	0,00	0,00	0,81
E	22,15	0	0,11	0,41
Бағандар бойынша сома	**57,69**	**0,21**	**1,55**	**3,25**

Осылайша, есептеудің осы қадамының нәтижесінде біз ақпараттық қауіпсіздік және КБ бойынша жобаларды бөлу бойынша баламаны іске асыру барысында пайдаланылатын ресурстардың әрқайсысының жиынтық саны туралы мәліметтер аламыз: $Q^{j1}(X_1) = 57{,}69;\ Q^{j2}(X_1) = 0{,}21;\ Q^{j2}(X_1) = 0{,}21;\ Q^{j4}(X_1) = 3{,}25.$ Әрі қарай $\mu_{Q^j}(X_n)$ анықтаймыз.

$Q^{j1}(X_1) = 57{,}69 > Q^{j^*} = 50$ және $Q^{j4}(X_1) = 3{,}25 > Q^{j^*} = 3$ болғандықтан, $\mu_{Q^1}(X_1) = \mu_{Q^4}(X_1) = 0.$

Мұнда $\mu_{Q^2}(X_1) = \mu_{Q^3}(X_1) = 1$, себебі ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік (РЖ) қамтамасыз ету жөніндегі жобаларға тартылған адам ресурстарының саны және ақпараттық қауіпсіздік және ОБИ киберқауіпсіздік (БШ) саласындағы жобаларды басқаруға арналған шығындар шектеудің төменгі шекарасынан аз $A^j = 2$.

Ұқсас есептеулер қалған екі k_1, k_2 және оптималдылық критерийлері үшін басқа критерийлер үшін де жүргізіледі.

Әрі қарай, формуланы (2.11) қолдана отырып, біз 2.1 кестеде қабылданған барлық k_1, k_2, k_3 критерийтар үшін $F_k(X_1)$ есептейміз, нәтижесінде, келесі мәндер алынады: $F_1(X_1) = 27{,}91$, $F_1(X_1) = 44{,}02$, $F_1(X_1) = 53{,}94$. $F_1(X_1), F_2(X_1), F_3(X_1)$ және $F_{\max k}$ формула бойынша (2.18) есептегеннен кейін по формуле (2.18) $\mu_{F_k}(X_1)$, табамыз, 2.6-кестені қараңыз.

2.6-кесте – $F_k(X_1)$, $F_{\max k}$, $\mu_{F_k}(X_1)$ - есептеу нәтижелері

Оңтайлылық критерийлері	$F_k(X_1)$	$F_{\max k}$	$\mu_{F_k}(X_1)$
k_1	27,91	72,86	0,551
k_2	44,02	79,56	0,412
k_3	53,94	80,54	0,661

Алынған шешімдердің әрқайсысы үшін тартымдылық (2.18) формуласы бойынша Беллман–Заде принципі негізінде есептеледі.

Сонда $\mu(X_1) = \max \min\left\{\mu_F(X_1), \mu_Q^j(X_1)\right\} = 0$, аламыз, себебі $\mu_{Q^1}(X_1) = \mu_{Q^4}(X_1) = 0$

Бастапқы популяцияның хромосомалары үшін (2.8-суретті қараңыз) есептеу нәтижелері 2.7-кестеде келтірілген.

X_2, X_3 хромосомалар (2.13)–(2.15) шектеулерді қанағаттандырмайтындықтан, олар үшін бейімделу функциясы (фитнес функциясы) нөлге тең.

Іріктеу операторы ретінде біз осы процедураны қолданамыз. Алдымен μ_0. популяцияның жалпы бейімделуін табамыз, 2.7 кестесіндегі мәліметтерге сәйкес жалпы бейімделу: $\mu_0 = 0{,}2 + 0{,}34 + 0{,}5 = 1{,}04$. құрайды.

Содан кейін біз салыстырмалы μX_n. бейімделуді анықтаймыз. Бұл үшін әр шешімге $P(X_n)$. ықтималдық беріледі. $P(X_n)$. мәні оның тартымдылығының барлық шешімдер жиынтығы үшін тартымдылық сомасы қатынасына тең:

$$P(X_n) = \mu(X_n) \Big/ \left(\sum_{n=1}^{m} \mu(X_n) \right) \qquad (2.22)$$

Бастапқы популяцияның хромосомаларына салыстырмалы бейімделуді есептеу нәтижелері 2.8-кестеде көрсетілген.

2.7-кесте – Бастапқы популяция хромосомаларының бейімделуі

Хромосома нөмірі	Хромосомадағы екілік реттілік	Салыстырмалы бейімделу
1	$X_1 = 1011\ \ 0011\ \ 1101\ \ 0011\ \ 1011$	0
2	$X_2 = 0100\ \ 0110\ \ 1101\ \ 0101\ \ 0000$	0
3	$X_3 = 1000\ \ 0000\ \ 1010\ \ 1101\ \ 0000$	0
4	$X_4 = 0111\ \ 0011\ \ 0111\ \ 0001\ \ 1010$	$0{,}2 / 1{,}04 = 0{,}1923$
5	$X_5 = 0101\ \ 1010\ \ 0010\ \ 0110\ \ 1001$	$0{,}34 / 1{,}04 = 0{,}3269$
6	$X_6 = 1111\ \ 0011\ \ 1000\ \ 0101\ \ 1011$	$0{,}5 / 1{,}04 = 0{,}4807$

2.8-кесте – Барлық хромосомалардың нәтижесі

Хромосома	Критерий k_1 (Бәсекеге қабілеттілік деңгейін арттыру және жаңа нарықтар)					Критерий k_2 (Инновацияларды дамыту және бизнес процестерге цифрлық технологияларды енгізу)					Критерий k_3 (ақпараттық технологиялар шығындарын төмендету)					$\mu(Xn)$
	μ_{Q_i}				μ_F	μ_{Q_i}				μ_F	μ_{Q_i}				μ_F	
	μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		μ_{Q_1}	μ_{Q_2}	μ_{Q_3}	μ_{Q_4}		
1	0	1	1	0	0,411	0,491	1	1	1	0,551	0,250	1	1	0,303	0,662	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	1	1	0,8	0,2	0,521		1	0,9	1	0,481	1	1	0,303	0,60	0,60	0,2
5	1	1	1	1	0,461	1	1	1	1	0,412	1	1	1	1	1	0,34
6	1	1	1	0,6	0,582	1	1	1	1	0,661	0,50	1	1	1	1	0,5

Зерттеу барысында пропорционалды іріктеу (немесе рулетка схемасы) қолданылды. Пропорционалды таңдау хромосомаларды ата-ана ретінде таңдау ықтималдығын анықтауға мүмкіндік береді. Іріктеу хромосомалардың салыстырмалы бейімділігі негізінде жүзеге асырылады. Схема «рулетка» деп аталды, өйткені процесс барысында сенімділік аралығы ата-аналарды таңдау рулетка секторын таңдауға ұқсас [70, 117-б.].

Рулетка *m* бір рет іске қосылады, яғни бастапқы популяция үшін шешімдер санына пропорционалды.

$P(X_n)$ ықтималдық, шын мәнінде, *n*-шешім үшін рулетка секторының көлеміне сәйкес келеді.

Бұдан әрі орындалады: іріктеу жасаймыз. Таңдау процесінде барлық шешімдер ауыстырылады. Таңдау үшін интервалда біркелкі таралуы бар кездейсоқ *m* сандарды құру керек (0,1). Содан кейін өрнектің көмегімен жаңа шешімдер жиынтығын құруға болады:

$$X_n^{new} = \begin{cases} X_n, if\ W_n < P(X_n); \\ X_{n+1}, if\ P(X_n) < W_n < P(X_{n+1}), \end{cases} \quad (2.23)$$

мұнда $n = 1,2,...,m.$ үшін W_n – кездейсоқ шешімдер саны.

Мысалы, 2.9-кестеде көрсетілген популяция алты кездейсоқ сандардың көмегімен құрылды.

2.9-кесте – Рулетка схемасын қолдану нәтижесінде пайда болған популяция

Нөмір	Популяция хромосомасындағы екілік реттілік	Салыстырмалы бейімделу
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1000 0101 1101	0,5
4	0111 0011 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

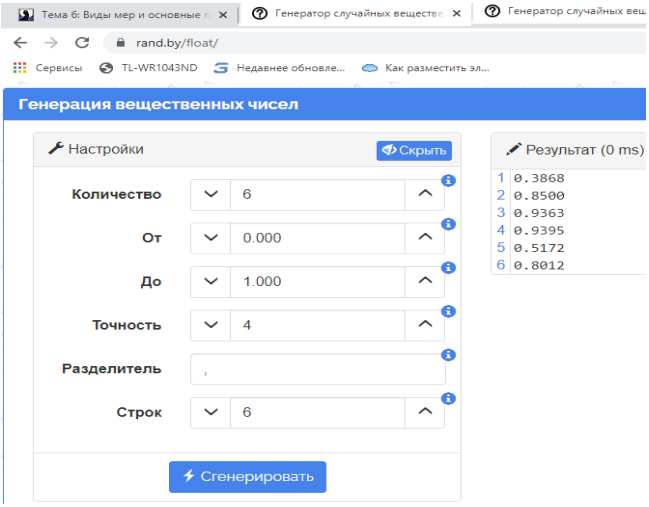
Таңдау операторын қолдану нәтижесінде жаңа жиынды аламыз. Кроссинговерге қатысатын хромосомаларды таңдау үшін келесі қадамдарды орындау қажет:

1-қадам) Алты кездейсоқ санды өңдеу, генерациялау үшін онлайн қызметті пайдаланған, 2.12-суретті қараңыз.

2-қадам) Кездейсоқ сан 0,8-ден аз болса, біз таңдаймыз деген ережеге сүйене отырып хромосомаларды таңдаңыз. Бұл мән комбинацияның ықтималдығынан $0{,}8$ аз болғандықтан қабылданады.

3-қадам) Хромосомаларды таңдағаннан кейін кездейсоқ кроссинговер нүктесін таңдаймыз, мысалы, кездейсоқ сандарды онлайн режимінде өңдеу қызметін қолдана отырып.

3-қадам) Кроссинговер процесін орындаймыз.



2.12-сурет. Кездейсоқ сандар генераторының онлайн жұмысының мысалы

2.12-сурет – Кездейсоқ сандар генераторының онлайн жұмысының мысалы

Мысалы, генерация нәтижесінде мұндай кездейсоқ сандар интервалда алынды (0,1):

$x_1 = 0{,}7532;\ x_2 = 0{,}9307;\ x_3 = 0{,}5325;\ x_4 = 0{,}1211;\ x_5 = 0{,}1732;\ x_6 = 0{,}8345.$

Сонда ата-аналық хромосомалардың жұптары $X_1 - X_3$ және $X_4 - X_5$ болады $X_1 - X_3$ жұбы үшін қиылысу нүктесі 12. $X_4 - X_5$ жұбы үшін - 8. Қиылысу нүктелерінен кейін орналасқан хромо-

сомалардың бөліктерінің (яғни биттер) орнын өзгертеміз. Кроссинговер процесі және ұрпақ алған нәтиже 2.10-кестеде көрсетілген.

2.10-кесте – Кроссинговер процесі

Ата-аналар	Кроссинговер			Ұрпақтары
$X_1 - X_3$				
1111 0011 1000 01011101	1111 0011 1000 ~0101 1101	→	1111 0011 1000 ~ 0101 1101	1111 0011 1000 0101 1101
1111 0011 1000 0101 1101	1111 0011 1000 ~0101 1101	→	1111 0011 1000 ~ 0101 1101	1111 0011 1000 0101 1101
$X_4 - X_5$				
0111 0011 0111 0001 1010	0111 0011 ~ 0111 0001 1010	→	0111 0011 ~ 0010 0110 1001	0111 0011 0010 0110 1001
0101 1001 0010 0110 1001	0101 1001 ~ 0010 0110 1001	→	0101 1001 ~ 0111 0001 1010	0101 1001 0111 0001 1010

Егер кроссинговер процесінде қалыптасқан ұрпақтар (2.13)–(2.15) шектеулерді қанағаттандырса, онда біз оларды ата-аналардың орнына қайта жазамыз. Егер шектеулер (2.13)–(2.15) қанағаттандырылмаса, онда біз ата-аналық шешімдерді өзгеріссіз қалдырамыз. Тиісінше, хромосомалардың жаңа ұрпағы 2.11-кестеде көрсетілгендей болады.

2.11-кесте – Жаңа ұрпақ

Нөмірі	Популяция хромосомасындағы екілік реттілік	Салыстырмалы бейімделу
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1000 0101 1101	0,5
4	0101 1001 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

Мутацияның генетикалық алгоритмде іріктеу процесіне қалай әсер ететінін қарастырайық. [70, с. 40-48] сәйкес, мутация – бұл

хромосома биттерінің бірінің инверсиясы. Бұл бит те кездейсоқ таңдалады. Мутация операторы мутацияның төмен ықтималдығын ескере отырып жұмыс істеді делік. Мысалы, үшінші хромосоманың 17-ші битін мутациялады: Популяцияның үшінші хромосомасындағы бастапқы екілік реттілік: 1111 0011 1000 0101 1101

Мутациядан кейінгі популяцияның үшінші хромосомасындағы екілік реттілік: 1111 0011 1010 0101 0101 Бұл хромосоманың бейімделуі да артты. Егер бастапқыда ол 0,5 болса, мутациядан кейін ол 0,56 болды. Осылайша, генетикалық алгоритм жұмысының нәтижесінде пайда болған популяция 2.12-кестедегідей болады. Осымен генетикалық алгоритм циклы аяқталды. Циклдар саны жұмыста қарастырылған мақсатты функцияларды оңтайландырудың дәлдігіне әсер етеді, сондықтан жұмыстың келесі тарауларында есептеулерді автоматтандыру үшін генетикалық алгоритм тарауында сипатталған бағдарламалық қамтамасыз ету әзірлеуге назар аударылады.

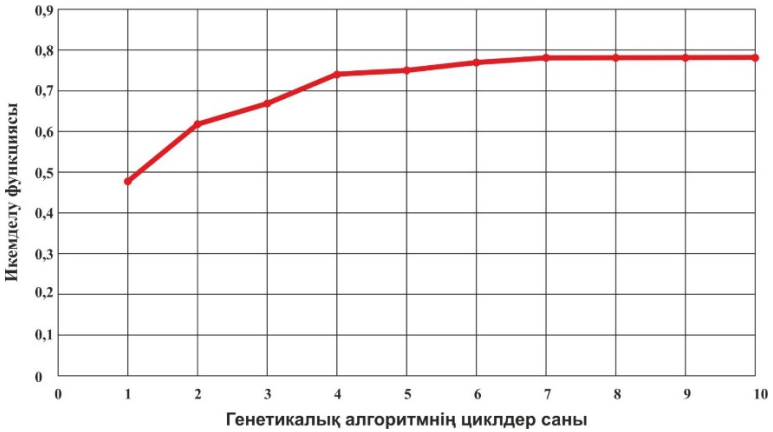
2.12-кесте – Алынған популяция

Нөмірі	**Популяция хромосомасындағы екілік реттілік**	**Салыстырмалы бейімделу**
1	1111 0011 1000 0101 1101	0,5
2	0101 1001 0010 0110 1001	0,34
3	1111 0011 1010 0101 0101	0,56
4	0101 1001 0111 0001 1010	0,2
5	0101 1001 0010 0110 1001	0,34
6	1111 0011 1000 0101 1101	0,5

2.8 және 2.12-кестелерінің деректерін салыстырмалы талдаудан көрініп тұрғандай, тіпті бір ғана итерация кезінде популяция сапасы екі еседен астам өсті.

Қазіргі және алдыңғы қадамдардағы фитнес функциясының ең үлкен мәндерінің арасындағы айырмашылық 0,01-ден аз болған кезде алгоритм тоқтайды, 2.7-суретті қараңыз. Бірінші циклден кейін бұл айырмашылық 0,5 болды, жаңа цикл қажет. Тест барысында $0,78 \approx 0,8$ деңгейінде фитнес функциясының оңтайлы мәнін алу үшін генетикалық алгоритм 7-ден 9-ға дейін цикл өтті.

2.13-суретте жобаланған генетикалық алгоритм үшін фитнес функциясының (бейімделу функциясының) өзгеру кестесі көрсетілген. 8 циклден кейін фитнес функциясы өзінің мағынасын сақтайды және генетикалық алгоритм жұмысын жалғастырудың мәні жоқ.



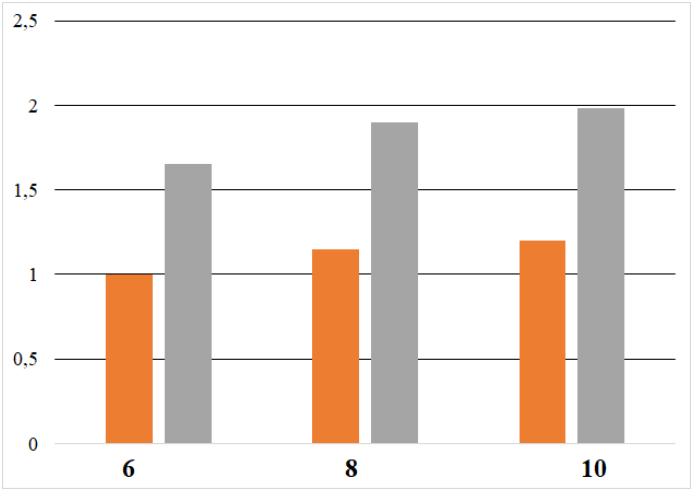
2.13-сурет. Әзірленген құрама генетикалық алгоритм үшін икемделу функциясының өзгерту кестесі

Алынған шешімді тексеру үшін қарапайым сұрыптау әдісін қолдана отырып, есепті шешудің бақылау есептеулері жасалды. Қарапайым сұрыптау аясында хромосомалардың барлық мүмкін мәндері үшін фитнес функциялары есептелді. Хромосомалардың жалпы саны бойынша 20 айнымалыдан тұратын шешім матрицасының мүмкін күйлерінің саны бірден мүмкін болатын шешімдердің 50%-дан астамы (2.13) - (2.15) шектеулерді қанағаттандырмайтындығын атап өтті. Осы баламалар үшін есептеулер жүргізілген жоқ. Қалған хромосомалар үшін фитнес функциясы іріктеліп алынды. Екі әдіс те ұқсас нәтиже берді, бірақ шешім табу үшін қарапайым іздеу үшін шамамен 65% көп уақыт қажет болды, 2.14-суретті қараңыз. Уақыт шкаласы шартты бірліктерде ұсынылған (мысалы, минуттарда немесе он минутта, өйткені әртүрлі процессорлары бар ЖК қолданған кезде есепті шешу уақыты дұрыс болмауы мүмкін). Осылайша, фитнес функциясы 0,8 мәніне сәйкес келетін шешім оңтайландыру есебінің шешімі болады.

Осылайша, генетикалық алгоритм көмегімен алынған шешімге сүйене отырып, келесі қорытынды жасауға болады:

Компания (кәсіпорын) өзінде бар ресурстарды ескере отырып, ақпаратты қорғаудың кешенді жүйелерін өрістету жөніндегі жұмыстарды ұйымдастырған жөн, өйткені бұл жұмыстар қорғаныс тарабы мен шабуыл жасаушылардың ресурстарының әртүрлі үйлесімдері кезінде ақпараттандыру объектісі осалдығын сипаттайтын мақсат функцияда (2.10) пайдаланылатын *a* параметр мәнінің 80%-ына дейін қамтамасыз етеді;

Кешенді ақпаратты қорғау құралдарына ғана бөлінетін ресурстарды одан әрі қайта бөлу ұсынылмайды, өйткені бұл ақпараттандыру объектісіндегі ақпараттың осалдығын одан әрі төмендетуге әкелмейді.



2.14-сурет. Әзірленген генетикалық алгоритм көмегімен және қарапайым сұрыптау әдісі үшін 6,8,10 хромосомасына есепті шешуге арналған уақыт шығындарын салыстыру диаграммасы (ш.б.-де)

Оң нәтижені барынша арттыру үшін А жұмыс түрінің шеңберінде (кешенді ақпаратты қорғау құралдарын жобалау, әзірлеу және өрістету): сәйкестендіру және аутентификациялау; қолжетімділікті басқару; ақпаратты машиналық тасығыштарды қорғау; басып кіруді анықтау; виртуалдау ортасын қорғау; және т.б.

жүйелерге қаражат инвестициялау қажет. Бұл қорытынды $x_{11} = x_{12} = x_{14} = 1$. Генетикалық алгоритмнің жұмысын көрсету үшін сынақ мысалына негізделген. А $x_{13} = 0$ болғандықтан, бұл ұсыныс ақпараттандыру объектісі ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы жобаларды басқаруға қаражат салуды болдырмау болып табылады, өйткені бұл іс-шаралар күрделілік-тиімділік қатынасы бойынша шектеулерді қанағаттандырмайды. Басқа бастапқы деректер үшін жағдай басқаша болуы мүмкін және бұл бағыт ақпаратты қорғау құралдары мен киберқауіпсіздікке инвестиция салу басымдыққа ие болады.

Сол сияқты, 2.1-кестесіндегі тізімнен басқа жұмыстар үшін ойлау тізбегін құруға болады. Егер бастапқы деректерде көрсетілген ресурстардың әр түрін қолдануды қарастыратын болсақ, онда тек адам ресурсының артықшылығы бар деп айтуға болады. Қалған ресурстар белгіленген анық емес шектеулер ауқымында болады.

Мұндай жүйелерді таңдау бойынша көп критерийлі есепті шешудің модельдері мен әдістерін азаматтық авиация жүйесін қолдану негізінде де ұйымдастыруға болады. Монографияның келесі тараулары осы зерттеулерге арналған. Бұл есепті шешу көбінесе n параметрдің шекаралық көрсеткіштерін анықтауға бағытталған, өйткені көптеген түйіндерден тұратын көп контурлы жүйелерді құруға келгенде қорғаныс өнімділігі соған байланысты болады. Әрбір мұндай тораптарда ақпарат өңделуі, сақталуы, берілуі, жаңаруы мүмкін. Тиісінше, қорғаныс тараптарының ресурстары шектеулі немесе минималды болған жағдайда қорғаныс құралдары мен тетіктерін таңдау жеке есеп болып табылады.

2.3. 2-тарау бойынша қорытындылар

Зерттеу нәтижесінде ақпараттандыру объектісі объектілерінде ақпараттық ресурстардың осалдығы мен қауіптерді іске асырудан келтірілген залалды сипаттайтын модельдің мақсатты функциясын таңдау негізделген.

Бөлшек-сызықтық функциялар материалдық тасымалдаушыларда сақталатын ақпараттың осалдығын сипаттайды, мұнда ақпаратты қорғауға, сондай-ақ ұйымдастырушылық және инженерлік-

техникалық іс-шараларға және қорғаныс құралдарына бөлінетін ресурстардың ұлғаюы, қорғаныс жақтары ресурстары мәндерінің бастапқы аймағында осалдықтың монотонды, пропорционалды түрде азаюына және нәтижесінде ақпараттандыру объектісі үшін келтірілген залалдың азаюына әкеледі.

Бөлшек-сызықты емес функциялардың кедергілерді жеңу үшін айтарлықтай ресурстар қажет болатын компьютерлік жүйелерде таратылатын ақпараттың қасиеттерін көрсететіні анықталды. Мақсатты функцияға кіретін және ақпараттандыру объектісіндегі ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстар тізбесіне тәуелді ұтымды $a, n,$ параметрлерді (бұл параметрлер ақпараттандыру объектісі үшін ақпаратты қорғау құралдары шығындарының өнімділігіне немесе жалпы жағдайда нақты ақпаратты қорғау құралдары тиімділігі көрсеткіштерінің және оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасына сәйкес келеді) іздеу есепін шешу үшін және кешенді ақпаратты қорғау құралдарын өрістету, ақпараттық қауіпсіздік (ақпараттық қауіпсіздікті қамтамасыз ету жүйесі) қамтамасыз ету жүйесін жетілдіру және т.б.) алғаш рет жаңғыртылған генетикалық алгоритмді пайдалану ұсынылды. Жаңғыртылған генетикалық алгоритмде қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді оңтайландырудың көп критерийліесепін шешу үшін Беллман-Заде қағидаты қолданылды. Бұл ақпараттандыру объектісі құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді оңтайландыруға және шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда ақпараттандыру объектісі қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік береді.

3 МОДИФИКАЦИЯЛАНҒАН ГЕНЕТИКАЛЫҚ АЛГОРИТМДІ ҚОЛДАНУ НЕГІЗІНДЕ АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫН ОРНАЛАСТЫРУДЫ ОҢТАЙЛАНДЫРУ БОЙЫНША ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ

3.1. Ақпаратты қорғау тарапының ресурстарын іріктеу, оңтайландыру және қайта бөлу есебін шешу үшін генетикалық алгоритмді дамыту

Әртүрлі АҚИ мен олардың ақпараттық-коммуникациялық жүйелеріне сәтті іске асырылған кибершабуылдардың саны мен күрделілігіне қарай қорғаныстың барлық контурларында ақпараттық қауіпсіздік және киберқауіпсіздік кешендерінің құрамын қалыптастырудың сапалы жаңа рәсімдеріне қажеттілік артады. Ақпараттық-коммуникациялық жүйе киберқауіпсіздік тиімді контурларын қалыптастырудың тұрақты есепі ақпаратты қорғау құралдары және киберқауіпсіздік құрамын оңтайландыру есептері бойынша көптеген зерттеулер жүргізгенін байқаймыз. Бұл зерттеулер, ең алдымен, көп критерийлі оңтайландыру есептерін шешуге байланысты сұрақтарға жауап беруге арналған, олар келесідей қасиеттерге ие: жеке ақпаратты қорғау құралдарын қолданудың рұқсат етілген аймағының күрделі конфигурациясы; қарастырылған функциялардың көп экстремалдылығы; функциялардың алгоритмдік тапсырмасы және т. б. Сонымен қатар, тиімді көп тізбекті киберқауіпсіздік жүйелерін құрудың нақты есептерінде шешімдер сирек бір критерий бойынша бағаланады. Сондықтан, мұндай есеплерде қолайлы парето-оңтайлы шешімдерді табу ғана емес, сонымен қатар шешім қабылдауш тұлғаларға ақпараттық-коммуникациялық жүйе киберқауіпсіздікке тиісті контурлары бойынша ақпаратты қорғау құралдарын объективті таңдауды ұсыну үшін алынған көптеген нұсқаларды жақындату маңызды. Ақпараттық-коммуникациялық жүйге деструктивті әсер ету әрекеттері санының өсуі жағдайында ақпаратты қорғаудың көп контурлы жүйелерін құрудың жоғарыда аталған есептерін шешу тек классикалық оңтайландыру процедураларын ғана емес, сонымен

қатар көптеген күрделі есептерді шешуде тиімді екендігі дәлелденген генетикалық алгоритмдерді қолдануды талап етеді [77, 78].

Генетикалық алгоритм тиімділігі олардың параметрлерін мұқият реттеу және бақылау арқылы анықталады. Бұл генетикалық алгоритмді ақпараттық-коммуникациялық жүйе контурлары бойынша ақпаратты қорғау құралдары тиімділігін қарапайым инженерлік есептеулерде қолдануды біршама қиындатады. Алайда, егер ақпараттық-коммуникациялық жүйе арналған ақпаратты қорғау құралдары құрамын таңдау бойынша дәстүрлі көп критерийлі оңтайландыру есепінен басқа, тәуекелдердің шамасын, сондай-ақ нақты активтер үшін (деректер базасы, білім базасы, пошта, сайт және т.б.) іріктелген ақпаратты қорғау құралдары құндық көрсеткіштерін қарастырса, генетикалық алгоритмді қолдану әбден орынды болады. Шешімді іздеу процедурасы шешім қабылдауды қолдаудың интеллектуалды жүйелерінің (шешім қабылдауды қолдау жүйесі) әлеуетін пайдаланса, тиімдірек болуы мүмкін, олардың есептеу ядросы іс жүзінде генетикалық алгоритмді қолдануға негізделген.

1 және 2 генетикалық алгоритм тарауларында көрсетілгендей, көп критерийлі оңтайландыру есептерін шешу кезінде қолданылатын іздеу эволюциялық әдістерінің нұсқалары болып табылады. Соңғы бірнеше жылда осы саладағы зерттеулерге көптеген жұмыстар арналды. Есепн, [79] модель сипатталған, оған сәйкес ақпаратты қорғау құралдары (дарақтар) элементтерінің популяциясы құрылады, онда оңтайландыру есебінде әр дарақ мүмкін шешімдердің біріне сәйкес келеді. Ең жақсы шешімді табу үшін авторлар өздерінің мақсатты функциясын қолданды. Жұмыста ұсынылған шешімдер іс жүзінде қалай және қай жерде нақты қолданылғаны көрсетілмеген.

[80, 81] еңбектерінде екі топқа жатқызуға болатын генетикалық алгоритм зерттелді. Бірінші топта екілік кодталған генетикалық алгоритм зерттелді. Екінші топта, тиісінше, қолданыстағы кодталған генетикалық алгоритм. Бұл жұмыстар бірінші топта рұқсат етілген шешімдер жиынтығында экстремалды мәнді іздеудің жоғары тиімділігіне қол жеткізуге болатындығын көрсетеді.

[82, 83] еңбектерінде модификацияланған генетикалық алгоритмді мұндай көп критерийлі оңтайландыру есептерінде қолдану ерекшеліктері қарастырылды. Генетикалық алгоритмнің стандартты генетикалық алгоритмнен салыстырмалы фитнес функциясымен

айырмашылығы мынада: алгоритм жұмыс істеп тұрған кезде фитнес функциясы ретінде ақпаратты қорғау құралдары тиімділігінің қосындысы қолданылмады, ол іс жүзінде хромосома болды, бірақ ақпаратты қорғау құралдарының шектеуші сипаттамаларына тиімділік қатынастарының қосындысы немесе тиімділік коэффициенті қолданылды. Генетикалық алгоритмнің ұқсас модификациясы іс жүзінде стандартты генетикалық алгоритм және сараң алгоритмнің бұзылуы болып табылады.

Ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдары құрамын таңдауды оңтайландыру есепін көп таңдаумен байланысты есептердің вариациясы ретінде қарастыруға болады [84, 85]. Бұл жұмыстарда ақпараттық-коммуникациялық жүйе контурларының компоненттерін орналастыруды оңтайландыру рюкзак комбинаторлық тапсырмасының белгілі бір модификациясы ретінде қарастырылады. Бұл тәсіл шешімді тұжырымдау мен түсіндірудің қарапайым формалдануымен ерекшеленеді. Алайда, авторлар генетикалық, қарапайым сұрыптау, адаптивті бағдарламалау және т.б. сияқты шешім алгоритмдерін толық шешуді және салыстыруды ұсынған жоқ.

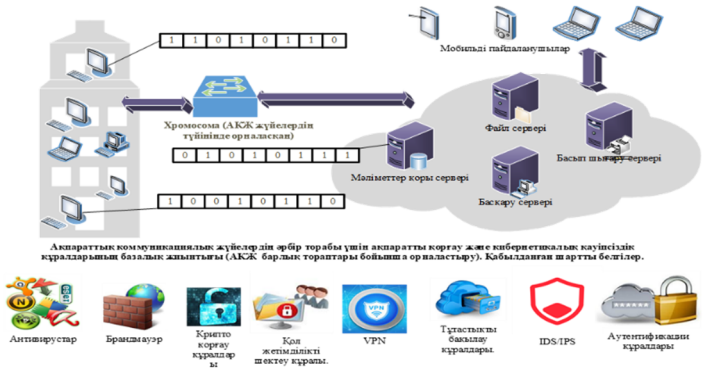
Алайда, мультипликативті рюкзак туралы тапсырма басқа кластарындағы заттармен бір ақпаратты қорғау құралдары класындағы заттарды ауыстыруға байланысты барлық мүмкіндіктерді көрсетпейтінін ескертеміз. Алайда, ауыстырылатын заттар балама функцияларды орындайды. Сондықтан объектілердің жалпы құнының орнына көптеген мақсаттарды көрсететін функцияны енгізу қажет. Бұл «рюкзактағы» заттардың өзара алмастырылуын немесе баламалылығын көрсету үшін жасалады.

Киберқауіпсіздік және ақпараттық қауіпсіздікті қамтамасыз ету тұрғысынан ақпараттық-коммуникациялық жүйе инфрақұрылымы 3.1-суретте көрсетілген.

Әдепкі бойынша, ақпараттық-коммуникациялық жүйе түйіндерінде стандартты ақпаратты қорғау құралдары орнатылған: антивирустар; брандмауэр; құралдар: 1) басып кіруді анықтау 2) криптографиялық АҚ; 3) қол жеткізуді шектеу; 4) тұтастықты бақылау; 5) аутентификация және т. б.

Әрине, нақты ақпараттық-коммуникациялық жүйе үшін тізім жеткіліксіздікке байланысты толықтырылуы немесе артықтығына байланысты қысқартылуы мүмкін.

NIST ұсыныстарында ақпараттық-коммуникациялық жүйеде киберқауіпсіздік және ақпараттық қауіпсіздікті қамтамасыз етудің архитектурасы, негізгі осалдықтары және ерекшеліктері егжей-тегжейлі сипатталған. Алайда, бүгінгі күні нақты ақпараттық-коммуникациялық жүйенің барлық ерекшеліктерін, киберқауіпсіздікті қамтамасыз ету тетіктерін талдауды және қауіптердің салыстырмалы спектрін ескере отырып, ақпараттық-коммуникациялық жүйе түйіндері бойынша ақпаратты қорғау құралдары мен киберқауіпсіздік орналастырудың оңтайлы нұсқасын іздеу процесінде біржақты шешім қабылдауға қабілетті әмбебап тәсіл жоқ екенін ескереміз. Нәтижесінде, мұндай тәсілді құру туралы есеп туындайды. Бұл жағдайда алынған шешім бірнеше маңызды мүмкіндіктермен ерекшеленуі тиіс. Біріншіден, ол нақты ақпараттық-коммуникациялық жүйенің құрылымына сүйене отырып, ақпараттық және киберқауіпсіздік контурларының түрлі нұсқаларын жобалауға мүмкіндік беруі қажет. Екіншіден, нақты қауіп-қатерлер кластарын ескере отырып, ақпаратты қорғау құралдарын таңдауды қамтамасыз етуі тиіс. Үшіншіден, шабуыл механизмдерінің эволюциясына негізделген бейімделу мүмкіндігі болуы керек, яғни ақпаратты қорғау құралдары мен киберқауіпсіздік жиынтықтарын таңдау және оңтайландыру үшін эволюциялық алгоритмдерді пайдалану қажет. Бұл тәсіл ақпараттық-коммуникациялық жүйе түйіндері үшін ақпаратты қорғау құралдарын таңдаудың жалпыға бірдей әмбебап әдістерін қолданудың мүмкін еместігін көрсетеді және нақты жағдайға бейімделген шешімдерді талап етеді.



3.1-сурет. Киберқауіпсіздікті қамтамасыз ету тұрғысынан ақпараттық-коммуникациялық жүйе ақпараттандыру объектісі инфрақұрылымы

3.1-суретте көрсетілген ақпаратты қорғау құралдары тізбесі толық емес. Бизнес-процестердің ерекшелігіне, ақпараттандыру объектісіндегі ақпараттық ресурстардың күрделілігіне байланысты бұл тізім кеңеюі мүмкін. Қорғаудың аппараттық-бағдарламалық құралдары, мысалы, SIEM системалар (ақпараттық қауіпсіздік оқиғаларын (дабылдарын) нақты уақытта талдау процестерін қамтамасыз ететін және осы оқиғаларға айтарлықтай залал басталғанға дейін ден қоюға мүмкіндік беретін), (инсайдерлік ақпараттың жария болуын болдырмау мақсатында қызметкерлердің іс-әрекеттерін қадағалауға және талдауға мүмкіндік беретін) және т. б., сондай-ақ ұйымдастырушылық және басқа да шаралар есебінен, мысалы, киберқауіпсіздік бойынша мерзімді оқу-жаттығулар өткізу, персонал жұмысын бақылау жүйелері есебінен айтарлықтай кеңейтілуі мүмкін.

Жоғарыда айтылғандарға сүйене отырып, ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдарының оңтайлы конфигурациясын (бұдан әрі – жиынтық) таңдау процесінде көп таңдау есебін (мысалы, антивирустар, желілік экрандар, басып кіруді анықтау құралдары және т.б.) шешу үшін генетикалық алгоритм қолдану мүмкіндігін қарастырамыз.

Біз шешімді кодтаудың келесі табиғи әдісін қолданамыз. Бастапқыда барлық құралдар, ал біздің жағдайда тиісті кластара жатқызылған ақпаратты қорғау құралдары тақырыпты ұсынудың екілік форматында нөмірленеді. Содан кейін әр хромосоманы $(x_1, x_2, ..., x_n)$ вектор түрінде көрсетуге болады. Бұл векторда егер бұл ақпаратты қорғау құралы ақпараттық-коммуникациялық жүйе түйінінде болса (рюкзак немесе мультирюкзак үшін бөлім) x_i элемент (яғни, *i*-ген) 1-ге тең (бірлік) немесе қарама-қарсы жағдайда - 0. Әрбір $(x_1, x_2, ..., x_n)$ булдік вектордың рұқсат етілген шешімді кодтай бермейтіні даусыз. Бұл ақпараттық-коммуникациялық жүйе түйініндегі элементтер жиынтығына (ақпаратты қорғау құралдары) шектеулердің болуымен байланысты. Мысалы, пайдаланушылардың мобильді құралдарында (ноутбуктер, планшеттер және т.б.) басып кірулерді анықтау құралдарын олардың қымбат болуына және есептеу ресурстарына сұранысқа байланысты олардың толық ауқымды нұсқасында орналастырудың мәні жоқ.

Сонымен қатар, түйіннің сыйымдылығы қаражаттың жалпы құнымен шектеледі (рюкзактың сыйымдылығы немесе біздің жағдайда интегралды көрсеткіш (ақпаратты қорғау құралдары), олар сол жерде орналасуы мүмкін. Сонымен қатар, жұмыстың екінші тарауында айтылған ресурстарды қайта бөлуге байланысты шектеулерді ескеру қажет.

Әрбір осАОБ ақпараттандыру объектісі үшін мұндай есеп қоюдағы фитнес функциясы осы осАОБ есепті шешудің сенімді нұсқасына «жақындық» дәрежесін сипаттайды. Фитнес функциясының мәні неғұрлым көп болса, шешім қалаған максимумға жақын болады.

Содан кейін түйінге арналған фитнес функциясын (ақпараттық-коммуникациялық жүйе үшін ақпаратты қорғау құралдары орналастыру нүктесі) келесідей пайдалануға болады:

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} w_i \cdot x_i,$$

мұнда w_i – сапа индексі немесе белгілі бір ақпаратты қорғау құралдары үшін қажетті мақсаттарға қол жеткізу дәрежесі деп аталатын класс немесе нақты ақпаратты қорғау құралдарының интегралдық көрсеткіші [86, 87].

Сондай-ақ, интегралдық көрсеткіш белгілі бір ақпаратты қорғау құралдарының маңызды сипаттамаларының сапасының жалпыланған көрсеткіші ретінде түсіндірілуі мүмкін. Интегралды көрсеткіш ақпараттандыру объектісі үшін ақпаратты қорғау құралдарына арналған шығындардың *a,b,n* өнімділік параметрлерімен немесе жалпы жағдайда нақты ақпаратты қорғау құралдарының тиімділік көрсеткіштері мен оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасымен тікелей байланысты.

Әзірленген алгоритмде сапа индексі немесе белгілі бір ақпаратты қорғау құралдары үшін қажетті мақсаттарға қол жеткізу дәрежесі интегралдық көрсеткіш ақпаратты қорғау құралдары ретінде қабылданды [88]. Авторлар ЖТС-ті белгілі бір ақпаратты қорғау құралдарының маңызды сипаттамалары сапасының жал-

пыланған көрсеткіші ретінде түсіндіреді. Бұл ретте, интегралдық көрсеткіші ақпаратты қорғау құралдары параметрлерінің бөлінген жеке көрсеткіштер кеңістігіндегі мінсіз сипаттамаларға жақындық дәрежесі ретінде есептелген деп есептейміз [88, б.150-154]. ақпаратты қорғау құралдары интегралдық көрсеткішін есептеу үшін, әдетте, келесі тәуелділікті қолданамыз:

$$IND_j = \sum_{i=1}^{k} \beta_i \cdot a_{ij}, \qquad (3.1)$$

мұнда β_i – i-ші ақпаратты қорғау құралдары бағалау үшін пайдаланылатын өлшемнің салмағы (мысалы, файерволдар үшін мынадай өлшемдерді пайдалануға болады: ішкі шабуылдардан қорғауға арналған брандмауэр тесті; сыртқы шабуылдардан қорғауға арналған брандмауэр тесті; осал қосымшаларға жасалған шабуылдардан қорғауға арналған дербес IDS/IPS тесті; құжаттаманың болуы және т. б.);

a_{ij} – шабуылдардың әр класы үшін түйіннің берілген қорғаныс деңгейіне жету дәрежесі;

k–ақпараттық-коммуникациялық жүйе түйінінің белгілі бір түріне арналған ақпаратты қорғау құралдары кластарының саны.

Ақпараттандыру объектісінің тиісті контурларына таралған ақпаратты қорғау жүйелері мен жеке ақпараттық қауіпсіздік құралдарын талдай отырып, жұмыстың алдыңғы тарауларында көрсетілгендей, барлық нысандар жүйе үшін бірдей мәнге ие емес және бірдей дәрежеде қорғалуы керек екенін атап өткен жөн. Бұл жағдай генетикалық алгоритмді көп критерийліесеп үшін қолдану тұрғысынан ақпаратты қорғау құралдары интегралдық көрсеткішті есептеуге өз ерекшеліктерін жүктейді.

Шынында да, ақпараттық-коммуникациялық жүйеде орналасқан кейбір объектілердің жұмыс істеуі бизнес-процестерді жүзеге асыру үшін өте маңызды, мысалы, дерекқор серверлері немесе қосымшалар сервері. Олардың істен шығуы дереу барлық ақпараттық-коммуникациялық жүйе ақпараттандыру объектісіне әсер етеді және төтенше жағдайларда оның қабылданбауына әкеледі.

Басқа жүйелер онша маңызды емес, олардың бүкіл ақпараттандыру объектісінің жұмысына әсер ету дәрежесі онша үлкен емес. Мысалы, кәдімгі компьютердің істен шығуы бизнес-процестерді толығымен тоқтатуға әкелмейді. Ақпараттық-коммуникациялық жүйенің маңызды және маңызды емес түйіндері үшін олардың қорғаныс құралдары қажет болса да, оларда орналасқан ақпараттық ресурстардың маңыздылығы мен сыншылдығына байланысты оларды қайта бөлу де маңызды рөл атқарады. Осыған байланысты ЖТС есептеу нақты ақпаратты қорғау құралдары аса маңызды параметрлерінің сапа сипаттамаларын жалпылаудың қарапайым процедурасынан аса күрделі есеп болып табылады.

Демек, интегралды көрсеткішті сапалы сипаттау үшін осы қорғаныс құралын орнату жоспарланған ақпараттандыру объектісі түйінінің барлық қасиеттерін ескеру қажет. Атап айтқанда, мыналарды ескеру қажет: түйіннің маңыздылығы; ақпараттық-коммуникациялық жүйеде осы түйіннің маңыздылығы; түйін үшін қорғаныс шараларын жүзеге асыру әдісі.

Бұл тізімде «сыншылдық» қасиеті басым болады. Ол түйіннің бүкіл ақпараттық-коммуникациялық жүйеге әсер ету дәрежесін анықтайды.

«Маңыздылық» сияқты қасиет олардың жалпы интегралдық көрсеткіштегі нақты ақпаратты қорғау құралдары параметрлерінің салмағын анықтайды. Яғни, бұл интерпретациядағы маңыздылық ақпараттық қауіпсіздік жүйесінің функцияларының қайсысының кему ретімен түйін үшін маңыздырақ, ал қайсысы маңызды емес екенін ғана анықтайды. Осылайша, түйіндегі ақпаратты қорғау құралдарының «маңыздылығын» анықтау үшін олардың функционалдық сипаттамаларын басымдықтардың маңыздылығына қарай орналастыру керек. Мысалы, антивирустық бағдарламалық қамтамасыз ету үшін интегралдық көрсеткішті сипаттауда зиянды бағдарламалық қамтамасыз ету анықтау көрсеткіші маңыздырақ, ал антивирустық сигнатураларды күніне 2 немесе 1 рет жаңарту жиілігі онша маңызды емес. «Түйін үшін қорғау шараларын іске асыру» қасиеті тиісті ақпаратты қорғау құралдары параметрінің жай-күйі туралы ағымдағы деректердің болуын немесе болмауын анықтайды. (3.1) өрнектегі ақпаратты қорғау құралдары жиынтығындағы заттарды сапалы бағалау

үшін β_i нақты мән немесе шамамен қолданылуы маңызды емес. Бұл β_i параметр ең алдымен β_i сандық бағалау мен объектінің біржақты сәйкестігін жүзеге асыратындығына байланысты. Іс жүзінде, объектілерді бағалау процесінде бағалау көбінесе шындыққа қарағанда пессимистік сипатта болады. Осылайша, интегралды көрсеткіштің β_i параметрі мен мәнін анықтаған кезде бағалау үшін β_i аралық бағалауды қолданған дұрыс деп айтуға болады.

Генетикалық алгоритм үшін $\tau(\beta_i)$ нақты мәндерді таңдағанда, жиынтыққа кіретін заттың әртүрлі сапалық бағалары арасындағы салмақ арақатынасын қалыптастыруға баса назар аударылады. Тиісті аралықтың шекарасындағы $\tau(\beta_i)$ мәндердің өзгеруі жиынтықтағы заттың сапалық бағасын қатайтады немесе керісінше әлсіретеді.

Жоғарыда айтылғандарды ескере отырып, ақпаратты қорғау құралдары интегралдық көрсеткіші келесі тәуелділіктер арқылы есептеуге болады:

$$IND_j = \sum_{i=1}^{k} \tau(\beta_i) \cdot a_{ij}, \qquad (3.2)$$

мұнда

$$\tau(\beta_i) = \begin{cases} \tau_1, \beta_i \in \lfloor b_{1_1}, b_{1_2} \rfloor \\ \tau_2, \beta_i \in \lfloor b_{2_1}, b_{2_2} \rfloor \\ \quad \ldots \\ \tau_j, \beta_i \in \lfloor b_{j_1}, b_{j_2} \rfloor \end{cases},$$

b_{j_1}, b_{j_n} – ақпараттық-коммуникациялық жүйе түйініндегі ақпаратты қорғау құралдары жиынтығындағы пәнді бағалау шкаласының сол және оң жақтары.

Осылайша, (3.2) қатынасы объектіні бағалаудың сандық баламалары жиынындағы β_i параметрлердің сапалық бағалауларын сипаттайтын сандық эквиваленттер жиынының бейнесіне сәйкес келеді.

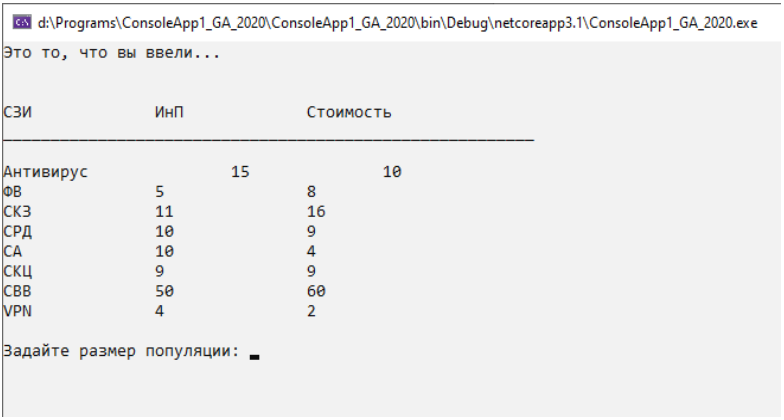
Рюкзак есебін шешу үшін классикалық генетикалық алгоритмді пайдалану жағдайында қарапайым кроссинговер мен мутация операторларын қолданумен байланысты есеп туындауы мүмкін екенін ескереміз. Егер бір нүктелі кроссинговер операторын қолданса, онда таңдалған ата-аналық хромосомалардан қате шешімді кодтайтын ұрпақ пайда болуы мүмкін. Шын мәнінде, логикалық вектор ақпараттық-коммуникациялық жүйе түйініндегі ақпаратты қорғау құралдары жиынтығын сипаттайтын жағдайға тап болу мүмкін, ол үшін интегралдық көрсеткіш берілген деңгейден бірнеше есе асады.

Сол сияқты, тұрақты мутация операторын қолдану хромосоманың пайда болуына әкелуі мүмкін, ол тапсырма үшін жарамсыз шешімді кодтайды.

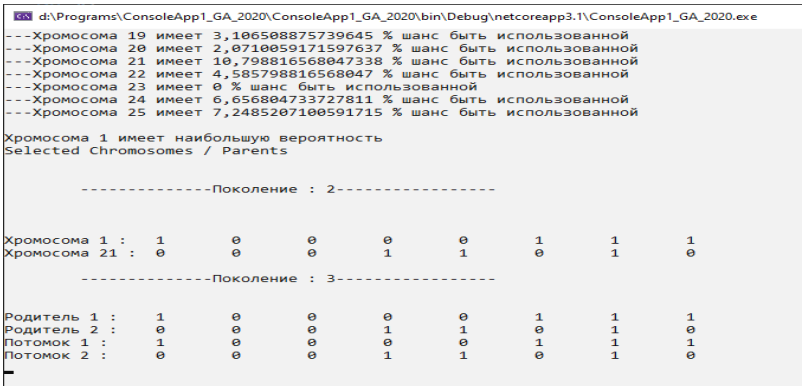
Егер алынған хромосомаларды түзету қолданылса, жоғарыда аталған қиындықтарды болдырмауға болады. Түзету келесі процедураны жүзеге асырудан тұрады. Алынған хромосомада биттердің жарамсыз кодталуы бар, кездейсоқ жеке гендерді таңдаймыз. Бұл таңдалған (1) гендер рұқсат етілген хромосома алынғанша нөлдік (0) гендерге ауыстырылады.

Сол сияқты мутация нәтижесінде алынған хромосомаларға түзету жүргіземіз. Ақпараттық-коммуникациялық жүйе түйіндері бойынша ақпаратты қорғау құралдары іріктеу процесінде генетикалық алгоритм қолдануға арналған консоль қосымшасының интерфейсі төменде келтірілген.

3.2-суретте бастапқы деректері бар қосымшаның терезесі, ал 3.3-суретте модельдеу нәтижелері бар терезе көрсетілген. Қорғаныс құралдарының элементтерінің немесе кластарының саны 8-ге тең, яғни NIST ұсынған барлық қорғаныс кластары үшін хромосомаларды іріктеу жағдайы модельденеді. Ұсыныстарға сәйкес, NIST [13, б.7, 14, б. 10] түйіндерде ақпаратты қорғау құралдарының барлық кластары орналасуы керек, 3.1-суретті қараңыз: вирусқа қарсы бағдарламалық қамтамасыз ету (Антивирус); құралдары - файервол (ФВ); криптографиялық қорғау (КҚ), қолжетімділікті шектеу (ҚЖШ), аутентификация (АҚ), тұтастығын бақылау (ТБҚ), басып кіруді анықтау (БАҚ) құралдары; VPN (VPN). Бағдарламаның листингі А қосымшасында келтірілген.



3.2-сурет. Генетикалық алгоритм көмегімен ақпараттық-коммуникациялық жүйе түйіні үшін ақпаратты қорғау құралдарын таңдауға арналған бастапқы деректер тізбесі бар терезе



3.3-сурет. Генетикалық алгоритм көмегімен ақпараттық-коммуникациялық жүйе түйіні үшін ақпаратты қорғау құралдары іріктеуді оңтайландыру процесін модельдеу нәтижелері бар терезе

Генетикалық алгоритм жұмысы келесі жағдайларда аяқталады: 1) фитнес-функцияның мәндері неғұрлым бейімделген особь-тарға және бірнеше жүйелі популяцияларда сәйкес келеді; 2) ұрпақтардың алдын ала келісілген санына қол жеткізілгенде. генетикалық алгоритмнің тағы бір кемшілігі - қажетті шешім

фитнес функциясының жергілікті максимумына сәйкес келетін, бірақ сонымен бірге локальді максимумға сәйкес келмейтін кезде оның жұмысын мерзімінен бұрын аяқтауы мүмкін. Монографияның екінші тарауында көрсетілгендей, бұтақтар мен шекаралар әдісіне негізделген алгоритмдерде бұл кемшілік жоқ. Алдыңғы бөлімдерде айтылғандай, бұтақтар мен шекаралар әдісі экспоненциалды күрделілікке ие және үлкен өлшемді тапсырмаларда қолдану мүмкіндігі шектеулі болса да, ол іздеу процедурасына үлкен дәлдік бере отырып, генетикалық алгоритмді толықтыра алады.

Жоғарыда айтылғандарды ескере отырып, қорғау тарапының ресурстарын іріктеу, оңтайландыру және қайта бөлу есебін шешу үшін генетикалық алгоритм модификациясы болып табылатын және бұтақтар мен шекаралар әдісі элементтерімен толықтырылған құрамдас алгоритмді (немесе түрлендірілген алгоритмді) қолдану ұсынылады.

Құрама әдісті қолданудың мәні бірінші кезеңде есепті шешу үшін генетикалық алгоритм қатысады. Екінші кезеңде генетикалық алгоритм көмегімен табылған шешімді бұтақтар мен шекаралар әдісі есебінен жақсартуға болады. Генетикалық алгоритм көмегімен түйінде (рюкзакта) ақпаратты қорғау құралдары жиынтығын қалыптастыру мүмкіндігі табылды. Жинақ бірден оңтайлы бола бермейді. Бірақ генетикалық алгоритм арқылы алынған кез-келген шешім сияқты, жиынтықтың табылған нұсқасы $(ch_1, ch_2, ..., ch_k)$ хромосома түрінде кодталады, ол 1 және 0-ден тұрады, онда $k-$ түйіндегі ЖҚҚ заттарының саны, 3.1суретті қараңыз. Әрбір торапта орналасқан ақпаратты қорғау құралдары олардың интегралдық көрсеткіші кему тәртібімен нөмірленеді. Мысалы, қол жеткізуді бөлу құралдары VPN-ге қарағанда жоғары орналасқан. Егер хромосомада бит 1-ге сәйкес келсе, онда тиісті ақпаратты қорғау құралдары ақпараттық-коммуникациялық жүйе түйінінде орналасқан деп санаймыз, егер 0 болса, онда болмайды. Іс жүзінде «сараң алгоритм» жиі қолданылады, оған сәйкес ең құндыны рюкзактарға салу керек [77, б.63]. Соңғы h- элементтерді $(ch_1, ch_2, ..., ch_k)$ жолдан алып тастаймыз. Нәтижесінде $(ch_1, ch_2, ..., ch_{k-h})$ жолды аламыз. Бұл жол ақпараттық-коммуникациялық жүйе түйінін (рюкзакты) толтыру нұсқасына

сәйкес келеді, онда түйінді толтырған және $n-h$ үлкен нөмірлері бар барлық заттар рюкзактан шығарылады.

Содан кейін $(ch_1, ch_2, ..., ch_{n-h})$ жолды h санмен биттермен (гендермен) толықтыруға болады. Нәтижесінде түйінді толтырудың жаңа нұсқасын аламыз. Бұл жаңа нұсқада генетикалық алгоритммен табылған шешіммен салыстырғанда түйін (рюкзак) үшін жоғары интегралдық көрсеткіші бар. Сонымен қатар, ШБӘ қолдана отырып, $(ch_1, ch_2, ..., ch_{n-h})$ жолды жалғастырудың ең жақсы нұсқасын таба аласыз. Шынында да, $(ch_1, ch_2, ..., ch_{k-h})$ жолда ақпараттық-коммуникациялық жүйе түйінінде жиналған ақпаратты қорғау құралдары бар. Бұл түйіннің бос бөлігінің сыйымдылығы түйінге (рюкзакқа) орналастырылған заттардың интегралдық көрсеткіші мөлшеріне сәйкес азайғанын білдіреді. Демек, IND' интегралдық көрсеткіші (сыйымдылығы) және C' құны бар жаңа рюкзак бар деп санаймыз, мұнда

$$IND' = IND - \sum_{i=1}^{k-h} a_i \cdot ch_i, \tag{3.3}$$

$$C' = \sum_{i=1}^{k-h} c_i \cdot ch_i, \tag{3.4}$$

мұнда $IND -$ ақпаратты қорғау құралдары интегралдық көрсеткіші.

Осылайша, генетикалық алгоритм көмегімен ақпараттық-коммуникациялық жүйе түйініне (рюкзакқа) ақпаратты қорғау құралдарын іріктеу кезеңін іске асырғаннан кейін, тапсырманы аз көлемді рюкзакқа қойдық, оны аз заттармен толтыру қажет. Енді ШБӘ қолдануға болады. Біз h биіктігі бар екілік ағаш саламыз. Әр шыңға 1 және 0-ден тұратын k ұзындық сызығы сәйкес келеді.

Жолдағы бірліктер түйінде орналасқан ақпаратты қорғау құралдары нөмірлерін көрсетеді. Екілік ағаштың тамыры h биіктікке ие. Түбірге $(ch_1, ch_2, ..., ch_{k-h}, 0, ..., 0)$ жолы сәйкес келеді. k биіктіктің шыңына $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, ..., 0)$ жолы сәйкес келеді. Сонда $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 1, 0, ..., 0)$ және $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, 0, ..., 0)$ жолдар тікелей ұрпақтарға сәйкес келеді және мұнда $l = 2, 3, ..., h$.

Ұрпақ жолдары ақпаратты қорғау құралдары түйінін толтырудың «жақын» нұсқаларын кодтайды. Ұрпақтар бір-бірінен ерекшеленеді, өйткені бірінші жағдайда түйінде $n-h$ нөмірі бар зат (ақпаратты қорғау құралдары) болады, ал екіншісінде болмайды. Барлық жолдар рұқсат етілмейді деп ойлаймыз, яғни максималды интегралдық көрсеткішті ескере отырып, түйінді толтырудың рұқсат етілген нұсқасын сипаттай алады. Сондықтан жарамсыз сызықтарға сәйкес келетін шыңдарда ұрпақтар болмайды. k биіктігі бар шыңға $(ch_1, ch_2, ..., ch_{k-h}, z_1, z_2, ..., z_{h-l}, 0, ..., 0)$ рұқсат етілген жол сәйкес келеді деп болжаймыз, мұнда $l = 2,3,..., h$ осы шыңға PS перспективасы сияқты параметрді есептейміз. Бинарлық ағаштың шыңдарының перспективасы деп ақпараттандыру объектісі қорғау тарабының шектеулі ресурстары жағдайында ақпараттық-коммуникациялық жүйе торабындағы ақпаратты қорғау құралдары жиынтық құнына салынған шектеу мөлшерін болжайтын боламыз. Шын мәнінде, параметр PS – бұл ақпараттық-коммуникациялық жүйе түйінінде орналасқан ақпаратты қорғау құралдарының максималды құны, егер оның $1,2,3,...,k-l$ нөмірі бар заттар түйінде орналасқандығы белгілі болса, анықтауға болады. PS параметрін келесідей есептеледі:

$$PS = \sum_{i=1}^{k-h} c_i \cdot ch_1 + \sum_{j=1}^{h-l} c_{k-h+j} \cdot z_j + \\ + \left(IND - \sum_{i=1}^{k-l} a_i \cdot ch_1 - \sum_{j=1}^{h-l} a_{k-h+j} \cdot z_j \right) \cdot \frac{c_{k-l+1}}{a_{k-l+1}} \quad (3.5)$$

Сонда екілік ағаштың шыңының бірінші деңгейі үшін PS параметрді келесідей есептейміз:

$$PS = \sum_{i=1}^{k-h} c_i \cdot ch_1 + \sum_{j=1}^{h-1} c_{k-h+j} \cdot z_j + c_k. \quad (3.6)$$

ШБӘ-ға сәйкес екілік ағаш жоғарыдан төменге қарай салынған. Құрылыстың әр кезеңінде келесі шың PS параметрді есептеу нәтижелеріне негізделген. Көрнекі мысал үшін біз антивирустық бағдарламалық қамтамасыз ету мен брандмауэр артық деп сеніп, тапсырманы сәл жеңілдетеміз. Windows 10 ОЖ соңғы нұсқасында антивирус әдепкідей орнатылады және оның жоғары рейтингтері қымбат коммерциялық антивирустық бағдарламаны пайда-

ланбауға мүмкіндік береді. Бұл брандмауэрге де қатысты. Сондықтан, иллюстрациялық мысалда біз тек 6 затты қалдырамыз: құралдар - криптографиялық қорғау (СКЗ), қол жетімділікті шектеу (ДӨЖ), аутентификация (СА), тұтастықты бақылау (СКЦ), басып кіруді анықтау (СВВ); VPN. Содан кейін ақпараттық-коммуникациялық жүйе түйініне арналған бастапқы мәліметтері бар кесте келесідей көрінуі мүмкін, 3.1-кестені қараңыз. Мысалдағы ақпаратты қорғау құралдары құны ұлттық валюталарға байланысты болмас үшін шартты бірліктерде немесе баллдарда көрсетілген. ақпаратты қорғау құралдарының интегралдық көрсеткіштері балдық бағалау негізінде, мысалы, www.anti-malware.ru сайты [89-95] деректері негізінде, сондай-ақ сараптамалық бағалау және өрнектің қолданылуын ескере отырып қабылданды (3.2).

3.1-кесте – ақпараттық-коммуникациялық жүйе түйіні үшін оңтайландыру есебін шешуге арналған бастапқы деректер

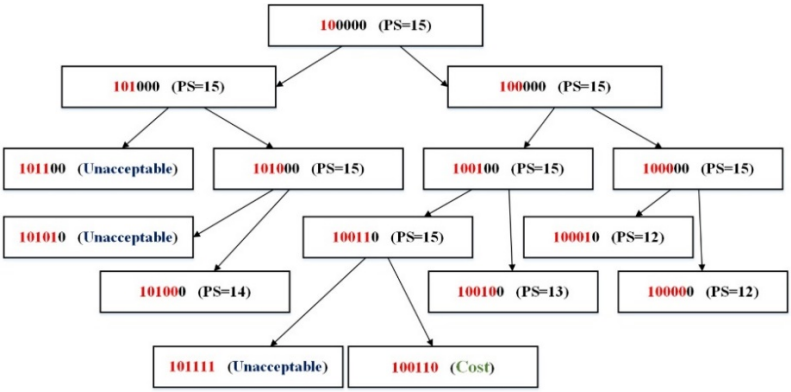
Пән нөмірі	**1**	**2**	**3**	**4**	**5**	**6**
ақпаратты қорғау құралының атауы	СКЦ	СКЗ	СВВ	СА	СРД	VPN
Шартты бірліктердегі құны	5.0	7.0	8.0	6.0	4.0	1.0
Интегралдық көрсеткіш	2	3	4	3	2	1

Генетикалық алгоритм жұмысының нәтижесінде ақпараттық-коммуникациялық жүйе ақпаратты қорғау құралдары түйінін ораудың белгілі бір нұсқасы анықталды делік. Нәтиже $ch = 101001$ хромосомаға жазылады. Біз интегралдық көрсеткіші тестінің мысалына 7-ге тең қоямыз (іс жүзінде бәрі таңдалған интегралдық көрсеткішін бағалау шкаласына байланысты. Мысалы, ол 1-ден 10-ға дейін немесе 1-ден 100-ге дейін өзгеруі мүмкін, [90]).

$IND = 7$ көрсеткіш үшін жиынтық интегралдық көрсеткіші 7-ге тең болады, ал түйіннің ақпаратты қорғау құралдары құны – 14 ш.б.

$h = 4$ параметр болсын. Содан кейін параметр жоғарыда сипатталған өзгертілген алгоритмді (генетикалық алгоритм + ШБӘ) қолдана отырып, 3.4-суретте көрсетілген екілік ағашты аламыз.

Біз екілік ағашты жоғарыдан бастаймыз, ол 100000 жолға сәйкес келеді. Жол 4 биіктікте орналасқан. Бұл жолдың параметрі PS = 15 тең. Бұл - түйіндегі барлық ақпаратты қорғау құралдарының интегралдық көрсеткіші қосындысына тең түйіндегі максималды интегралдық көрсеткіші.



3.4-сурет. Генетикалық алгоритм мен ШБӘ-ны біріктірген түрлендірілген алгоритм жұмысының иллюстрациясы

Соңғы h элементтерді (101001) жолдан алып тастаймыз. Нәтижесінде (100000) жолды аламыз. Бұл жол ақпараттық-коммуникациялық жүйе түйінін толтыру нұсқасына сәйкес келеді, онда түйінді толтырған және $k-h$ үлкен нөмірлері бар барлық заттар рюкзактардан шығарылады. 3.4-суретте рюкзакқа (түйінге) кірген ақпаратты қорғау құралдары кодтайтын жолдың сол жағындағы сақталған биттер қызыл түспен көрсетілген.

Әрі қарай, екілік ағаштың келесі деңгейінде (100000) жолды. көлемінде биттермен (гендермен) толықтырамыз. Содан кейін 3-ш биіктіктегі ұрпақтардың жолдары келесідей болады: (101000) және (100000). Ұрпақтың деректер параметрлері де $PS = 15$ болып табылады.

Біз ЕА-ны (101000) шыңнан салуды жалғастырамыз. Келесі екі ұрпақ қалыптасады, сәйкесінше – (101100) және (101000) жолдарымен ұсынылған. Бірінші ұрпақ, яғни (101100) жол рұқсат етілмейді, өйткені түйіндегі ақпаратты қорғау құралдарының жиынтық құны рұқсат етілген шекарадан асады (СКЦ (5.0)+СВВ (8.0)+СА (6.0)=19.0 ш.б.). Екінші ұрпақ, яғни $PS = 15$ жол болуы мүмкін және оның $PS = 15$.

(101000) жол, сонымен қатар, екі ұрпақты береді, сәйкесінше жолдар – (101010) және (101000). Сонымен қатар, егер бірінші жол ұрпағына жол берілмесе (СКЦ (5.0)+СВВ (8.0)+СРД (4.0)=17 ш.б.), онда екінші жол рұқсат етіледі, бірақ ол $PS = 15$ берілген мәннен аз, сондықтан ЕА-ның бұл бөлігін бұдан әрі құрудың мәні жоқ.

ЕА-ның жоғарғы жағына өтейік, ол (100000) жолда жазылған. Онікі *PS* =15. Жоғарыда сипатталғандай ойлана келе, (100000) жолдың ұрпақтарын талдаймыз. Бұл жол ұрпақтардың жолдарын құрайды -(100100) және (100000). Олардың параметрі - *PS* =15.

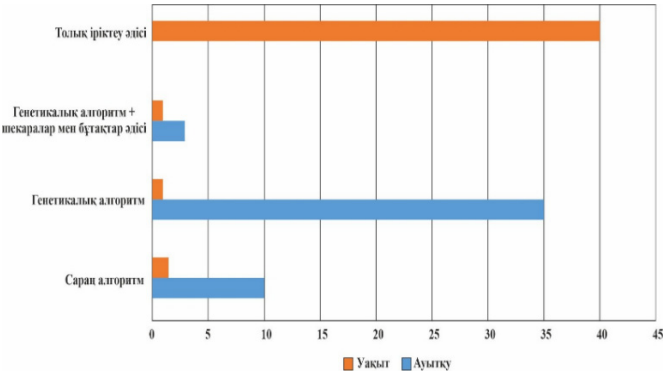
Тиісінше әрбір жол ұрпақтары өз ұрпақтарын береді. Ұрпақтардың әр -(100100) жолы да сәйкесінше -(100110) және -(100100) ұрпақтарын береді. Ал (100000) жол (100010) және (100000) ұрпақтарды береді. Алайда (101100), (101010) және (101111) шыңдарында ақпараттық қауіпсіздік көмегімен ақпараттық-коммуникациялық жүйе түйінін орау нұсқасына сәйкес келмейтін биттер болады.

Егер түйінде 1 зат (СКЦ) орналасса ал 2 зат (СКЗ) болмаса онда (100110) жолы шартты түрде ең жақсы деп есептеледі. Осылайша, генетикалық алгоритм артықшылықтары мен бұтақтар мен шекаралар әдісін біріктіретін өзгертілген алгоритмді қолдана отырып, тек генетикалық алгоритм арқылы алынған шешімді жақсартуға болады.

Бұл жағдайда модификацияланған (құрама) алгоритм ақпараттық-коммуникациялық жүйе түйіндерінің (рюкзактарының) саны едәуір үлкен болған жағдайда қызықты және классикалық әдістермен олардағы барлық ресурстарды қайта бөлуді оңтайландыру есебін қатар шешу өте қиын процесс [96,97]. Өзгертілген алгоритмнің жұмыс уақыты популяция мөлшері мен ұрпақтар санына тікелей пропорционалды, ал жиынтықтағы заттардың *k* санына көпмүшелік санға байланысты болады. Өзгертілген алгоритмнің жұмыс уақыты көбінесе *h* параметрдің көлеміне байланысты болады. Жоғарыда сипатталған сынақ мысалына және 3.2 және 3.4-суреттерінде көрсетілген нәтижелерге ұқсас, *k* және *h* бөлшек мәндер үшін есептеу эксперименттері жүргізілді. Ұсынылған модификацияланған құрама алгоритмді (генетикалық алгоритм +ШБӘ) ұқсас есептер класын шешу үшін қолданылатын басқа классикалық алгоритмдермен салыстыру үшін классикалық генетикалық алгоритм, «сараң» (СА) және нақты толық санау (ТС) алгоритмімен салыстырмалы талдау жасалды. Жоғарыда аталған алгоритмдерді бағалау үшін жиынтықта 5-тен 150-ге дейін тақырып жиынтығы (ақпаратты қорғау құралдары) жасалды. Серияда 30 тәжірибе бойынша 5 серия өткізілді, 3.2-кестені қараңыз. Барлығы 150 есептеу тәжірибесі. Есептеу эксперименттері Inteli7 9750h (2.6 – 4.5 ГГц) процессоры бар компьютерде жасалды.

Жұмыстың екінші тарауында көрсетілгендей, ақпараттық-коммуникациялық жүйе түйіндеріндегі ақпаратты қорғау контурларының аппараттық-бағдарламалық компонентіне ғана емес, сонымен қатар ұйымдастырушылық шараларға да назар аудару маңызды болғандықтан, ақпараттық-коммуникациялық жүйені қорғау дәрежесін жоғарылату үшін жұмыс тізіміндегі заттар тест жинақтарына да енгізілді. Бұл жұмыстар да құны мен интегралды индикатормен сипатталуы мүмкін. 3.5-суретте және 3.2-кестеде алгоритмдердің салыстырмалы сынақтарының нәтижелері көрсетілген. 3.1-кестеде көрсетілген заттар тізбесіне қосымша: телефон желілерін қорғау құралдары; үй-жайларды виброакустикалық қорғау жүйелері; сөйлесуге арналған үй-жайларда кедергілер қою құралдары; түрлі арналар бойынша ақпараттың тарауын анықтау құралдары; бейнебақылау құралдары және т. б. енгізілді.

Толық сұрыптаудың дәл әдісін қолдана отырып алынған шешімдер дәлірек болды деп күтілуде. Бірақ мұндай алгоритмнің жұмыс уақыты, тіпті i7 процессорларын қолдануды ескере отырып, генетикалық алгоритм немесе генетикалық алгоритм +ШБӘ-ға қарағанда 17-25 есе көп.



3.5-сурет. Әртүрлі алгоритмдер үшін нақты шешімдерден орташа ауытқулар және шешім табу уақыты

Генетикалық алгоритм мен ШБӘ-ты біріктіретін модификацияланған алгоритм монографияның келесі бөлімдерінде толығырақ сипатталатын әзірленген бағдарламалық өнімнің есептеу ядросына кіреді.

3.2-кесте – Пәндер жиынтығын – ақпараттық-коммуникациялық жүйе түйіндеріне арналған ақпаратты қорғау құралдарын қалыптастырудың әртүрлі алгоритмдеріне арналған салыстырмалы тест нәтижелері

№ серия-дағы тәжірибе	Тест жиынты-ғындағы заттар саны - N	Алгоритмдер			
		Толық санау	Классикалық генетикалық алгоритм (популяция мөлшері 50)	«Сараң» алгоритм	генетикалық алгоритм+ ШБӘ (популяция мөлшері 50)
		Шешім уақыты, с			
1	5	1	1	1	1
2	10	1	1	1	1
3	15	600	1	1	1
4	20	720	1	1	1
5	35	1000	1	1	1
6	30	1300	1	1	1
7	35	1600	1	1	1
8	40	2200	1	1	1
9	45	4500	1	1	1
10	50	4900	1	1	1
11	55	6020	1	1	1
12	60	7990	1	1	1
13	65	8900	1	1	1
14	70	9400	1	1	1
15	75	10100	1	1	1
16	80	10690	1	1	1
17	85	11450	1	1	1
18	90	11990	1	1	1
19	95	12670	1	2	2
20	100	13300	1	2	2
21	105	13900	1	2	2
22	110	14200	1	3	2
23	115	14800	1	3	2
24	120	15220	2	4	3
25	125	15700	1	4	3
26	130	16300	3	5	4
27	135	16500	3	6	4
28	140	16900	3	7	5
29	145	17500	4	8	5
30	150	18000	5	10	6

Бұл кестеде нақты нәтижеден берілген ауытқу үшін 5% артық емес екені анық көрсетілген.

3.2. Ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, қорғау құралдарының интегралдық көрсеткіштерін және олардың құнын пайдалануды ескере отырып, генетикалық алгоритмді дамыту

Тапсырманы генетикалық алгоритм тұрғысынан ресімдейміз. Хромосома қорғаныс шараларының жиынтығы деп санаймыз (мысалы, қорғаныс объектісінде ақпараттық қауіпсіздік саясатын сақтау ережелері), соның ішінде ақпаратты қорғау құралдары. Жиын екілік сан түрінде кодталған. Егер санның екілік разряды (1) бірлікке тең болса, онда тиісті ақпаратты қорғау құралдары немесе тиісті нөмірі бар ақпаратты қорғау жөніндегі шара жиынтыққа енгізіледі. Содан кейін кодты өзгерту ауқымын келесідей ұсынуға болады:

$$G = (d_0 d_1 \ldots d_{NC})_2 = (0 \ldots 2^{NC})_{10}, \quad (3.7)$$

мұнда NC – оңтайлы жиынтыққа қосу үшін ықтимал қарастырылатын ақпаратты қорғау құралдары және қорғау шараларының саны; d_i – ақпаратты қорғау құралдары және/немесе қорғау шараларын жиынтыққа қосу.

Генетикалық алгоритм терминдерінде популяция әртүрлі хромосомалары бар үлгілерден тұрады. Популяция мөлшері ондағы үлгілердің максималды санымен шектеледі. Популяцияның әр данасын келесідей сипаттауға болады:

$$Ch = \{G, C, R\}, \quad (3.8)$$

мұнда G – популяциядағы генетикалық коды экземпляры;

C – ақпаратты қорғау құралдары және/немесе тиісті қорғау шараларының құны;

R – таңдап алынған ақпаратты қорғау құралдары және/немесе 2-тарауда қаралған тиісті қорғау шараларын ескере отырып, ақпаратты (немесе оның құпиялылығын, тұтастығын) жоғалтудың жиынтық тәуекелі.

Тәуекелді анықтау үшін алгоритмді өзгерту процесінде келесі болжам қолданылады. Белгілі бір ақпараттық-коммуникациялық жүйе үшін ақша эквивалентіндегі шығындардың абсолютті мәні элементтер -қауіптер, осалдықтар, ақпаратты қорғау құралдары тізбегіне байланысты. Сондықтан тәуекелдер саны - бұл қауіптер мен активтердің жиынтығы:

$$R = TH \cdot M, \tag{3.9}$$

мұнда TH – қауіптер саны, M – активтер саны.

(3.9) формуласында бірнеше қауіптердің үйлесуі, сондай-ақ ақпаратты қорғау құралдары арасындағы ішкі әсер ескерілмеген. Сондықтан ақпараттық-коммуникациялық жүйе үшін қауіптерді анықтаудың неғұрлым қолайлы әдісі шабуыл профильдерін жасауға негізделген әдіс болып табылады [86, 165-б]. Бұл әдіспен шабуыл профильдері әртүрлі қауіптердің үйлесімінен тұратын шабуылдар тізбегі ретінде қарастырылады. Сонда тәуекелдер санын келесі тәуелділікпен сипаттауға болады:

$$R = \left(2^{TH}\right)^{TA} \tag{3.10}$$

мұнда TA – шабуылдар саны.

Демек, берілген профиль үшін тәуекелдің шамасы сәтті шабуылдардан келтірілген жалпы залалдың мөлшері деп санауға болады.

Егер шабуыл кезінде тізбекті реакция болмаса, онда жалпы тәуекелдің мәні әрбір ақпараттық-коммуникациялық жүйе активі үшін зиянды математикалық күту ретінде ұсынылуы мүмкін:

$$r = \sum P_{i,j} \cdot D_{i,j}, \quad i = \overline{1, TH}, \; j = \overline{1, M}, \tag{3.11}$$

мұнда $P_{i,j}$ – *(j)* активке *(i)* қауіп төндіретін ақпараттық-коммуникациялық жүйе ақпараттық қауіпсіздік қақтығысының ықтималдығы;

$D_{i,j}$ – оқыс оқиғаға байланысты залалдың мөлшері (ақшалай баламада қабылданған).

(Ch) хромосома матрица түрінде ұсынылуы мүмкін. Содан кейін матрицаның жолдары орналастыру нүктелері болады, сәйкесінше бағандар – нақты ақпаратты қорғау құралдарын қамтитын құралдар класы (мысалы, антивирустық бағдарламалық қамтамасыз ету класы қарастырылған антивирустық бағдарламалардың барлық нұсқаларын қамтуы мүмкін: Avast, Avira, AVG, Bitdefender және т.б.). g_{ij} матрица элементі *i* түйінге орналастырылған *j* кластан ақпаратты қорғау құралының нөмірін көрсетеді. Егер $g_{ij} = 0$, онда *j* кластан *i* түйінде бірде-бір құрал пайдала-

нылмайды деп есептейміз, мысалы, вирусқа қарсы бағдарламалық қамтамасыз ету желіаралық экранда пайдаланылмайды.

Генетикалық алгоритм (Ch) хромосомасының қалыптасу схемасы 3.3-кестеде келтірілген.

3.3-кесте. Хромосоманың қалыптасу схемасы

Қарсы шаралар кластары. Желі тораптары	N_1	N_2	...	N_{NC}
K_1	g_{11}	g_{12}	...	g_{1NC}
K_2	g_{21}	g_{22}	...	g_{2NC}
...	...	...	...	...
K_{KC}	g_{KC1}	g_{KC2}	...	$g_{KC,NC}$

Мұндай форматта ұсыну хромосоманың және контекстінде шешілетін есептер деп K_{KC} және N_{NC} – тиісінше, түйіндеріндегі ақпараттық-коммуникациялық жүйе және ақпаратты қорғау құралдары түйіндерінің саны.

(R) тәуекелді есептеу үшін келесі модельді қолданамыз. Генетикалық код бойынша әрбір тасымалдаушы үшін тиісті ақпаратты қорғау құралдарын таңдаймыз.

Генетикалық алгоритмге $U-.$ пайдалылық функциясын енгіземіз: бұл функция жиынтықта таңдалған ақпаратты қорғау құралдары тиімділігін бағалау үшін қажет. Таңдалған ақпаратты қорғау құралдары шабуыл профиліне сәйкес келуі керек екенін ескертеміз. Өйткені, мысалы, шектеулі функционалдығы бар тегін антивирустық бағдарламалық қамтамасыз ету DoD/DDoS шабуылдарымен күресу үшін мүлдем пайдасыз екендігі түсінікті, ал ақпараттық-коммуникациялық жүйеге арналған қауіпсіздік саясатын сақтау жөніндегі нұсқаулар инсайдерлерден қорғамайды.

Онда $U-.$ пайдалылық функцияны келесідей беруге болады:

$$U(Ch) = R_0 - Ch.R, \qquad (3.12)$$

мұнда $Ch-$ ақпаратты қорғау құралдары жиынтығының данасы;

R_0- егер ақпаратты қорғау құралдарының тиісті жиынтығын

қолданбаса, ақпараттың жоғалуына байланысты тәуекелдердің шамасы;

$Ch.R-$ ақпаратты қорғау құралдарының тиісті жиынтығын $Ch.G.$ (данасын) қолдануды ескере отырып, тәуекелдер шамасы

Алайда, ақпараттық-коммуникациялық жүйені шабуылдардан қорғау бойынша қол жеткізілген тиімділік, тиісінше, ақпаратты қорғау құралдарына қосымша шығындарды талап етеді. Келесі қатынасты қолдана отырып, ақпаратты қорғау құралдарына шығындардың әсерін ескереміз:

$$U(Ch)=\left(R_0-Ch.R\right)\Big/_{Ch.C}, \qquad (3.13)$$

мұнда $Ch.C-$ ақпаратты қорғау құралдары жинағының құны.

(3.13) формула қатынас әрбір салынған құн бірлігіне ақпараттың жоғалу қаупін қалай азайтуға (немесе арттыруға) болатындығын көрсетеді.

Әрі қарай, біз алынған өрнектерді генетикалық алгоритмде қалай қолдануға болатынын қарастырамыз. Жоғары деңгейлі бағдарламалау тілдерінің синтаксисінде кроссинговер, мутация, таңдау функциялары келесідей болады.

Кроссинговердің функциясы - жаңа тасымалдаушылардың өнімі. Генетикалық алгоритм базасында шешім қабылдауды қолдау жүйесі бағдарламалық іске асыру процесінде кроссинговердің екі түрі қаралды. Бір нүктелі және n-нүктелі кроссинговерді қолдану мүмкіндіктері талданды. Осы екі түрді таңдау келесі ойларға байланысты. Бір нүктелі кроссинговерге негізделген стандартты тәсіл генетикалық алгоритм көмегімен шешім табуға болатын көптеген тапсырмаларға сәйкес келеді, алайда ақпараттық-коммуникациялық жүйе түйіндеріне арналған ақпаратты қорғау құралдары көп таңдау есептері үшін стандартты генетикалық алгоритм өте дәл болмайды [96]. Бұл хромосома біртұтас бөлінбейтін құрылым болмайтындығына байланысты. Бұл есепті шешуде хромосоманы ыдырау процедурасын қажет ететін жүйе ретінде түсіндіруге болады. Декомпозиция хромосоманы бөліктерге бөлуге мүмкіндік береді және әр бөлім ақпараттық-коммуникациялық жүйе түйіндерінің өзіндік класына сәйкес келеді.

Біз әр жұп үшін (PA) ата-аналардың ерекшеліктерін мұра ететін жаңа дана жасаймыз.

$$
\begin{aligned}
&func\ K(PA) := foreach\ Ch(X)\ from\ PA\ and \\
&foreach\ Ch(Y)\ from\ PA\ where\ Ch(X) != \\
&Ch(Y)\ do\ R.add(\{G : xor(Ch(Xi).G, Ch(Xj).G), C :, R :\}) \\
&return\ R.add(PA)
\end{aligned}
\tag{3.14}
$$

Әрі қарай, мутация функциясын, яғни генетикалық кодтың өзгеруін қарастырыңыз. Мутацияның екі түрін қарастырудың негізінде бірқатар маңызды болжамдар жатыр. Біріншіден, тұрақты мутация генетикалық алгоритмдерді жүзеге асыратын бағдарламалық жасақтаманың басым көпшілігінде қолданылады және классикалық тәсіл ретінде қарастырылады. Екіншіден, зерттеліп отырған есептің айнымалылары жоғары икемділікті талап етеді, сондықтан мұнда генетикалық алгоритмнің тиімділігі кроссинговерге қарағанда мутацияға көбірек тәуелді. Үшіншіден, бұл болжам ақпараттық-коммуникациялық жүйелердің киберқауіпсіздік контурларын қалыптастыруға қатысты есептердің өзіндік ерекшеліктерімен түсіндіріледі. Мұндай ерекшеліктердің қатарына хромосомалардың үлкен көлемі мен шешімді шектейтін факторлардың көп болуы жатады. Осы себептерге байланысты кездейсоқ элементтерді қамтитын ауыспалы мутацияны қолдану тиімді болып табылады. Бұл тәсіл әсіресе алгоритмнің бастапқы кезеңдерінде «рюкзак» типті оңтайландыру есептерінде ең қолайлы құрамды табу тұрғысынан артықшылық береді. Нәтижесінде, ауыспалы мутация есептің күрделілігін ескере отырып іздеу кеңістігін тиімдірек қамтуға мүмкіндік береді және алгоритмнің жалпы өнімділігін арттырады. Есептеу эксперименттері барысында мутацияның екі түрі қарастырылды. Бірінші түрі - тұрақты мутация. Бұл жағдайда 1% ықтималдығы бар хромосомадағы әр позиция инверттеледі. Екіншісі - ауыспалы мутация. Бұл жағдайда мутация ықтималдығы генетикалық алгоритмнің қазіргі қажеттіліктеріне байланысты болады. Мутация коэффициенті 1-6% аралығында болады. Салыстырмалы фитнес функциясы бар қарастырылып отырған генетикалық алгоритмде фитнес функциясы ретінде хромосома құрайтын ақпаратты қорғау құралдары тиімділігінің қосындысы емес, класқа кіретін ақпаратты қорғау құралдарының тиімділігі немесе интегралдық көрсеткіштерінің қосындысы қолданылды.

Ол үшін хромосомадағы екі екілік разрядты кездейсоқ түрлендіреміз:

$$func\ M(PA) := foreach\ Ch(X)\ from\ PA\ do\ Ch(X).G = \\ = xor(Ch(X).G, 1 << rand(0, NC)). \quad (3.15)$$

Онда таңдау функциясы, яғни ең жақсы тасымалдаушыны таңдау келесідей ұсынылуы мүмкін:

$$func\ \ S(PA) := return\ \ PA.sort(\ ).slice(1, K). \quad (3.16)$$

Жазбаны азайту және популяцияны азайту үшін тек (U) пайдалы функцияға қатысты үлкен нәтиже беретін K тасымалдаушыларды қалдыратынымызды ескертеміз.

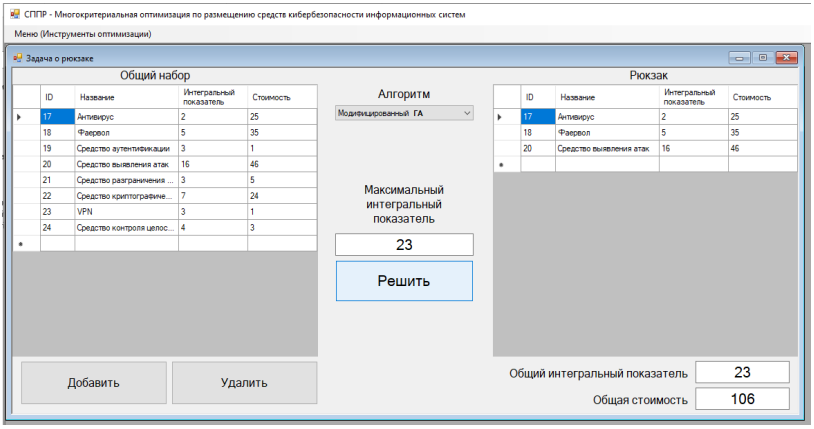
Таңдауды қолданар алдында популяция үшін $Ch(X).C$ және $Ch(X).R$ алдын-ала есептейміз. [78, б.67-72] сәйкес бастапқы популяция кем дегенде екі үлгіні қамтиды деп қабылданды. Сонда генетикалық алгоритмдегі әр дәуір жоғарыда қарастырылған негізгі функцияларды дәйекті қолданудан тұрады. Тиісінше, мынаны аламыз:

$$func\ \ E(\ ) := ((PA = K(PA), M(PA)), (P = S(PA))). \quad (3.17)$$

Шешім қабылдауды қолдау жүйесі жұмысының нәтижесінде тиісті кластан әрбір ақпаратты қорғау құралдарының интегралдық көрсеткіші және осы ақпаратты қорғау құралдарының құны негізінде ақпараттық-коммуникациялық жүйе түйіні үшін ақпаратты қорғау құралдарының оңтайлы жиынтығы айқындалады. ақпаратты қорғау құралдары кластары үшін интегралдық көрсеткіші талдау және есептеу негізінде оларды қалыптастырудың сараптамалық әдісін қолданбай ақпаратты қорғау құралдары кластары үшін салмақтық коэффициенттерге негізделген интегралдық көрсеткіші максималды мәні туралы түсінік жасауға болады. Шешім қабылдауды қолдау жүйесі есептеу ядросының бағдарламалық жасақтамасы, жоғарыда сипатталған модельдер, сонымен қатар Microsoft Visual Studio 2019 ортасында c# тілінде орындалған ақпараттық-ком-

муникациялық жүйе киберқауіпсіздік контурлары үшін ақпаратты қорғау құралдары жиынтығын құрудың оңтайлы стратегиясын табу есепін жүзеге асыратын алгоритм жұмыстың келесі тарауында толығырақ сипатталады. Сондай-ақ, оның нақты ақпараттандыру объектісіндегі тестілеу нәтижелері көрсетілген.

Шешім қабылдауды қолдау жүйесі тұжырымдамасы ақпараттық-коммуникациялық жүйенің қол жетімді архитектурасы, кластар мен ақпаратты қорғау құралдары жиынтығы негізінде, сондай-ақ бірінші кезеңде иерархияларды талдау әдісін (Т.Саати әдісі) қолдана отырып, генетикалық алгоритм +ШБӘ көмегімен ақпараттық-коммуникациялық жүйенің негізгі түйіндерінің әрқайсысында ақпаратты қорғау құралдарын орналастырудың оңтайлы нұсқасын қалыптастыру есепі шешіледі, 3.1-суретті қараңыз. Шешім қабылдауды қолдау жүйесі негізгі терезесі 3.6-суретте көрсетілген.



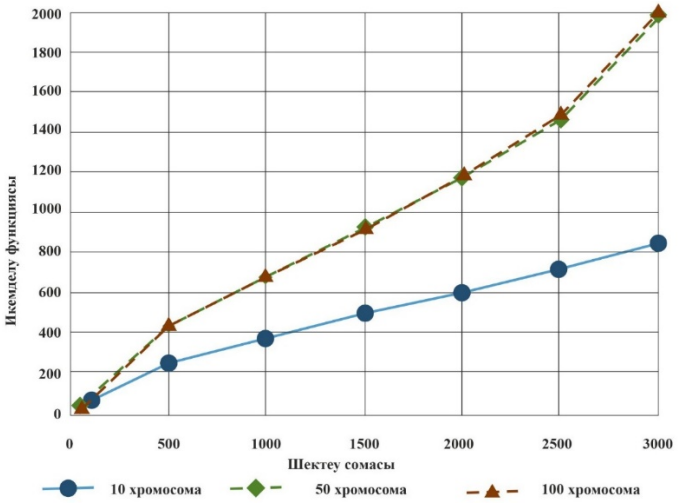
3.6-сурет. Шешім қабылдауды қолдау жүйесі модулі интерфейсінің жалпы түрі (модуль-түйін үшін ақпаратты қорғау құралдары құрамын таңдау есебін шешу үшін генетикалық алгоритм қолдану)

Кибернетикалық қауіпсіздіктің қажетті деңгейін қамтамасыз ету және есептеу параметрлерін реттеу үшін ақпараттық-коммуникациялық жүйе түйінінде қолданылуы мүмкін киберқауіпсіздік және ақпараттық қауіпсіздік (яғни хромосомалар) қамтамасыз етуге арналған заттардың жалпы жиынтығына қатысты барлық

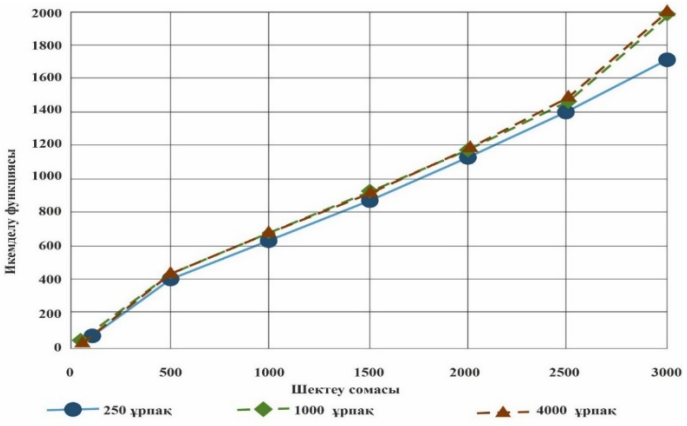
деректерді енгізгеннен кейін тікелей генетикалық алгоритм басталады. Сол үшін генетикалық алгоритм 25 хромосомадан тұратын популяцияны құрайды. Әрі қарай, әр хромосоманың фитнес функциясы (тиімділігі) есептеледі. Генетикалық алгоритмде k-нүктелі кроссинговер қолданылған. Шын мәнінде, k – ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдары орналастыру нүктелерінің саны.

Рюкзакқа арналған жиынтық, яғни талданатын ақпараттық-коммуникациялық жүйе түйіні 3.6-суреттегі форманың оң жағындағы кестеде көрсетілген. Яғни, іс жүзінде мультирюкзак қалыптастыру есебі шешіледі. Шешім қабылдауды қолдау жүйесі объектіге бағытталған тәсілді пайдалана отырып әзірленген. Модификацияланған генетикалық алгоритм +ШБӘ есептеу ядро мұнда қолданылған стандартты генетикалық алгоритмнен мынадай белгілермен ерекшеленеді: хромосомалар матрицалар түрінде ұсынылған, олардың элементтері ақпараттық-коммуникациялық жүйе түйіндеріндегі ақпаратты қорғау құралдары нөмірлеріне сәйкес келетін сандар болып табылады; *k*-нүктелі кроссинговер қолданылды. Ауыспалы мутация қолданылды, яғни мутация ықтималдығы қажеттілікке байланысты генетикалық алгоритм жұмыс барысында бейімделу түрінде өзгеруі мүмкін. Фитнес функциясы тиімділік коэффициенттерінің қосындысы ретінде ұсынылған. Бұл ретте, ақпаратты қорғау құралдары тиімділігінің дәстүрлі абсолютті көрсеткіштерінен (интегралдық көрсеткіште интеграцияланған) басқа, ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасы, сондай-ақ ақпаратты қорғау құралдарының әрбір класы үшін құндық көрсеткіштері ескеріледі.

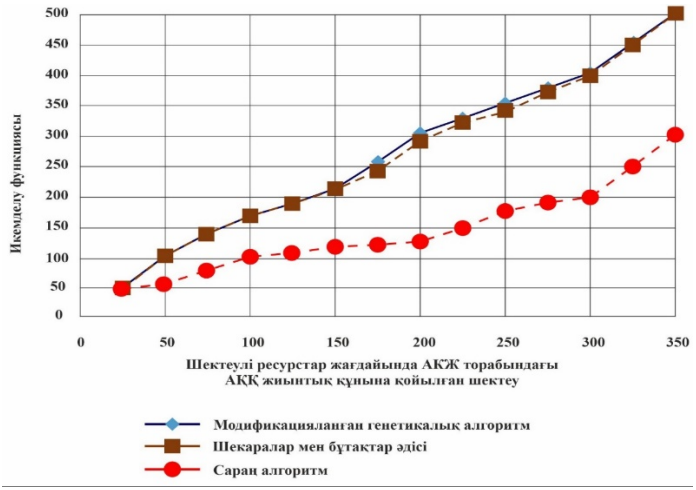
Ақпараттық-коммуникациялық жүйе түйіндері бойынша ақпаратты қорғау құралдары орналастыруды көп критерийтық оңтайландыру бойынша алгоритм мен шешім қабылдауды қолдау жүйесі барабарлығын тексеру үшін тиісті есептеу эксперименттері жүргізілді, 3.7–3.10-суреттерді қараңыз. Есептеу эксперименттері кездейсоқ құрылған ақпаратты қорғау құралдары жиынтығы үшін жүргізілді. Модификацияланған (құрама генетикалық алгоритм +ШБӘ), бұтақтар мен шекаралар әдісі және сараң алгоритмі жұмыстарының тиімділігі салыстырылды. 3.7-сурет – Популяциядағы хромосомалардың әртүрлі саны үшін алгоритмнің тиімділігі салыстыралды.



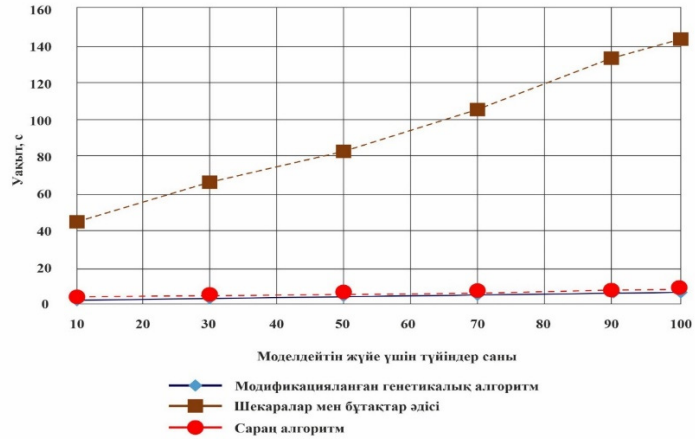
3.7-сурет. Популяциядағы хромосомалардың әртүрлі саны үшін алгоритмнің тиімділігін салыстыру



3.8-сурет. Әртүрлі ұрпақтар үшін алгоритмнің тиімділігін салыстыру



3.9-сурет. Шешім қабылдауды қолдау жүйесі пайдаланылатын алгоритмдердің тиімділігін салыстыру бойынша есептеу эксперименттерінің нәтижелері



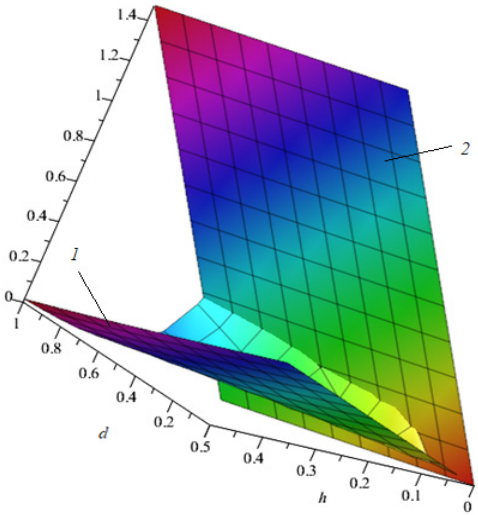
3.10-сурет. Алгоритмдер жұмыс уақытын салыстырғанда есептеу эксперименттер нәтижелері

3.7-суреттің графигінде популяциядағы хромосомалардың оңтайлы санын іздеу барысында ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғаудың оңтайлы жиынтығын іздеу есебін шешу үшін генетикалық алгоритм зерттеу нәтижелері көрсетілген.

Есептеу эксперименттері көрсеткендей, егер хромосомалардың саны үлкен болмаса (20-дан аз) оңтайлы нәтижеге қол жеткізу мүмкін емес. Алайда, олардың саны 22-25-тен асқан кезде алгоритмнің тиімділігі жоғарылаған жоқ. 500-ден астам есептеу эксперименттерінің сериясы негізінде алгоритмнің соңғы нұсқасы және оны бағдарламалық іске асыру үшін популяцияда 25 хромосоманы алу жеткілікті екендігі анықталды. Қарастырылып отырған генетикалық алгоритм+ШБӘ үшін ұрпақтардың оңтайлы санын іздеу барысында бірқатар есептеу эксперименттері жүргізілді, 3.8-суретті қараңыз. Тексеру барысында генетикалық алгоритм+ ШБӘ тиімділігі 450-500 ұрпақ шебінен өткеннен кейін артпайтыны анықталды. Бұл жағдай біздің шешім қабылдауды қолдау жүйесі үшін 500 ұрпақ санымен генетикалық алгоритм+ШБӘдағы ұрпақтар санын шектеуге негіз береді.Есептеу эксперименттері барысында генетикалық алгоритм + ШБӘ өте жоғары тиімділікпен, сондай-ақ жылдамдығымен ерекшеленетіні анықталды, 3.9, 3.10-сур. қараңыз. Генетикалық алгоритм+ШБӘ пайдалану кезінде есепті шешуге жұмсалған уақыт бұтақтар мен шекаралар әдісінің көрсеткіштерімен салыстырғанда шамамен 16-25 есе аз екендігі анықталды. Сараң алгоритм үстеме шектеулер мен айнымалылар санын ескере отырып, көп критерийліоңтайландыру есебін шешуге бейімделу тұрғысынан генетикалық алгоритмнен де, бұтақтар мен шекаралар әдісінен де айтарлықтай төмен. Осылайша, талдау әзірленген модельдер мен алгоритмнің сенімді екендігін және есептеу эксперименттерінің нәтижелері бірнеше рет практикалық іске асырулармен расталғанын көрсетеді. Генетикалық алгоритм және оның модификациясын тиімді пайдалану үшін генетикалық алгоритм +ШБӘ Комбинациясын қолдану арқылы алдымен ақпаратты қорғау құралдары жиынтығына ақпаратты қорғауға арналған ең өнімді құралдар мен металарды таңдау қажет екендігі көрсетілген. Жоғарыда қарастырылған интегралды көрсеткіш талданған ақпараттық-коммуникациялық жүйе түйіндері үшін қорғаныс құралдары мен шараларын таңдауда маңызды рөл атқарады. Бұл көрсеткіш монографиялық зерттеу контексінде нақты ақпаратты қорғау құралдарының аса маңызды сипаттамалары сапасының жалпыланған көрсеткіші ретінде түсіндіріледі. Интегралдық көрсеткіш ақпараттандыру объектісі үшін ақпаратты қорғау құралдары шығындарының өнімділік параметр-

лерімен тікелей байланысты болғандықтан (монографияның екінші тарауында қарастырылған), ақпараттық-коммуникациялық жүйе түйінінде ақпаратты қорғау құралдарының тиімді жиынтығын қалыптастыру, Егер белгілі бір ақпаратты қорғау құралдары үшін қажетті мақсаттарға қол жеткізу дәрежесі жоғары болса, қорғау тарапының ресурстарды бөлу бойынша артық шығындардан аулақ болады. Енді ақпараттық-коммуникациялық жүйе түйіні үшін ақпаратты қорғау құралдары іріктеудің оңтайландыру есепін шешу үшін модификацияланған генетикалық алгоритм қолданудың тиімділігі расталған кезде қауіптерді іске асырудан келтірілген залалды сипаттайтын мақсат функцияларды – өрнек (2.7), сондай-ақ қорғау түйіні ақпаратты қорғау құралдары инвестициялау стратегияларын таңдауды сипаттайтын функцияларды оңтайландыру үшін генетикалық алгоритм қалай жұмыс істейтінін көруге болады [91].

3.11-суретте екі беттің қиылысында құрылған мақсатты функцияны қалыптастыру мысалы көрсетілген: 1 – объектінің осалдығын сипаттайтын функция үшін [64, 156-б] және 2 – қорғау жағынан ақпаратты қорғау құралдарына инвестициялаудың оңтайлы стратегиясын сипаттайтын функциялар.



3.11-сурет. Екі беттің қиылысында құрылған мақсатты функцияны қалыптастыру: (1) – объектінің осалдығын сипаттайтын функция үшін және (2) - қорғау тарапынан ақпаратты қорғау құралдарына инвестициялаудың оңтайлы стратегиясын сипаттайтын функция.

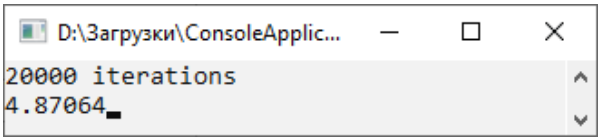
Осы функциялардың әрқайсысы үшін экстремумдарды іздеуді генетикалық алгоритмді қолдануға жүгіну арқылы ұйымдастыруға болады.

Мысалы, егер қорғаныс жағы үшін ақпаратты қорғау құралдарында инвестициялардың мөлшерін $const = 1$ (қорғаныс құралдары $-const = d$) тең қабылдайтын болсақ, онда фитнес функциясын (c++) модельдеу үшін ГА-ны келесі консольдік іске асыруды аламыз.

$$v(h,d) = r^n \Big/ \left(r^n + a\right), \text{ үшін } r = \left(h \Big/ d\right), \quad n = 3,\ a = 8\ .$$

Инвестиция кілт жоғалған (немесе бұзылған) сәтке дейін нәтиже бермейтін жағдай. Осыдан кейін криптожүйенің осалдығы күрт артады. *n* шамасы неғұрлым үлкен болса, кедергі шабуылдарға аз әсер ететін шекті мән соғұрлым үлкен болады. Сонымен қатар, қорғаныс жағы мен шабуылдаушылар ресурстарының арақатынасы шекті мәннен асқан кезде өсу аймағы соғұрлым тез артады.

Генетикалық алгоритм жүзеге асыру нәтижесінде келесідей нәтижеге қол жеткіземіз, 3.12-суретті қараңыз.



3.12-сурет. Бір айнымалы функцияны оңтайландыру нәтижесі (қорғаныстың тұрақты ресурстары кезінде шабуылдаушы тараптың ресурстары)

Алынған нәтиже шабуыл объектісі мен оның ақпараттық ресурстары осал болуы мүмкін екенін білдіреді, егер шабуылдаушы тарап осы ақпаратты қорғау құралдарын жеңуге өз салымдарын шамамен бес есе арттыруды қамтамасыз ете алатын болса. Мысалда ақпараттандыру объектісі үшін ақпаратты қорғау құралдары шығындарының өнімділік параметрлері қабылданады. Бұл мәндер сынақ болып табылады және зерттеу нәтижелері бойынша қабылданады [64, 150-160-б]. Бұл сынақ мысалында олар ақпаратты қорғаудың шартты құралдарының тиімділік көрсеткіштері мен

оларды сатып алу, қызмет көрсету, модернизациялау шығындарының коэффициенттерін сипаттайды.

Монографиялық зерттеудің 4-ші қорытынды тарауы ақпараттандыру объектісі үшін ақпараттық қауіпсіздік және киберқауіпсіздік көп контурлы жүйелерінің оңтайлы конфигурацияларын іздеу, сондай-ақ қолданыстағы қауіптердің өзектілігіне сүйене отырып, қорғау тарапының ресурстарын серпінді қайта бөлу жөніндегі есепті шешу үшін модификацияланған генетикалық алгоритм (генетикалық алгоритм +ШБӘ) қолдану бойынша шешім қабылдауды қолдау жүйесі әзірлеудің практикалық аспекті-леріне арналған.

3.3. 3-тарау бойынша қорытындылар

1. Ақпараттық-коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау құралдарының конфигурацияларының нұсқаларын іріктеумен және оңтайландырумен байланысты есепті шешу үшін генетикалық алгоритмді түрлендіру мүмкіндігі қаралды. Жұмыстың осы бөлімінде алынған нәтижелердің ғылыми жаңалығы генетикалық алгоритмде ақпаратты қорғау құралдары құрамын оңтайландыру үшін өлшемдер ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, ақпаратты қорғау құралдары интегралды көрсеткіштерін, сондай-ақ әрбір ақпаратты қорғау құралдары сыныбы үшін құндық көрсеткіштерді пайдалану ұсынылатындығында. Ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдары құрамын таңдауды оңтайландыру есебіндегі генетикалық алгоритм көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл өндірісте ақпаратты қорғау құралдарын ақпараттық-коммуникациялық жүйе - қорғаныс контурлары бойынша орналастыруды оңтайландыру рюкзактың комбинаторлық есепін өзгерту ретінде зерттеледі. Ұсынылған тәсіл ақпараттық-коммуникациялық жүйе түйіндерінің әрқайсысы үшін ақпаратты қорғау құралдары жиынтығын оңтайландыру жөніндегі көп критерийліесепті шешуге ғана емес, сонымен қатар ақпараттандыру объектісі киберқауіпсіздікке бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарапының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді.

Зерттеудің практикалық құндылығы ақпараттың жоғалуынан болатын қауіптердің жалпы мөлшерін, ақпаратты қорғау құралдары интегралды көрсеткіштерін, сондай-ақ ақпаратты қорғау құралдарның әрбір класы үшін құндық көрсеткіштерді ескере отырып, генетикалық алгоритмнің ұсынылған модификациясы негізінде шешім қабылдауды қолдау жүйесіне есептеу өзегі үшін серпінді қосылатын кітапхана түрінде модульді бағдарламалық іске асыру болып табылады. Генетикалық алгоритм және бұтақтар мен шекаралар әдісінің артықшылықтарын біріктіретін модификацияланған құрама алгоритмді іске асырудың ұтымды бағдарламалық алгоритмін таңдау бойынша есептеу эксперименттері жүргізілді. Әзірленіп жатқан шешім қабылдауды қолдау жүйесі үшін ұтымды нұсқа ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамаларын, ақпаратты қорғау құралдары интегралды көрсеткіштерін, ақпаратты қорғау құралдарының әрбір класы үшін құндық көрсеткіштерін ескеретін, сондай-ақ генетикалық алгоритм мен ШБӘ-ның барлық оң жақтарын біріктіретін генетикалық алгоритм модификациясын пайдалану керек екендігі көрсетілген. Модификацияланған генетикалық алгоритмді іске асыру ақпараттық-коммуникациялық жүйеге арналған киберқауіпсіздік құралдарын орналастырудың оңтайлы нұсқаларын іздестіруді жеделдетуге, сондай-ақ қорғау ресурстарын олардың шектеулілігі жағдайында қайта бөлу жөніндегі есепті шешуге мүмкіндік беретіні көрсетілді. Бұл артықшылық аппараттық және бағдарламалық жасақтаманың әртүрлі нұсқаларын және олардың ақпараттық-коммуникациялық жүйеге арналған комбинацияларын жылдам сұрыптауға ғана емес, бірақ кейінірек тарауда келтірілген модельдер мен алгоритмдерді қолданыстағы модельдермен және ақпараттық-коммуникациялық жүйе киберқауіпсіздік контурларының құрамын оңтайландыру алгоритмдерімен біріктіруге де жағдай жасайды. Модельдер мен алгоритмдердің мұндай бірігуі ақпараттық-коммуникациялық жүйе қорғанысын тез қалпына келтіруге мүмкіндік беретіндігі ықтимал.

4 ҚОРҒАУ ОБЪЕКТІЛЕРІ АРАСЫНДА РЕСУРСТАРДЫ БӨЛУДІ ОҢТАЙЛАНДЫРУ БАРЫСЫНДА ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУДЫҢ МОДУЛЬДІК ЖҮЙЕСІН ӘЗІРЛЕУ

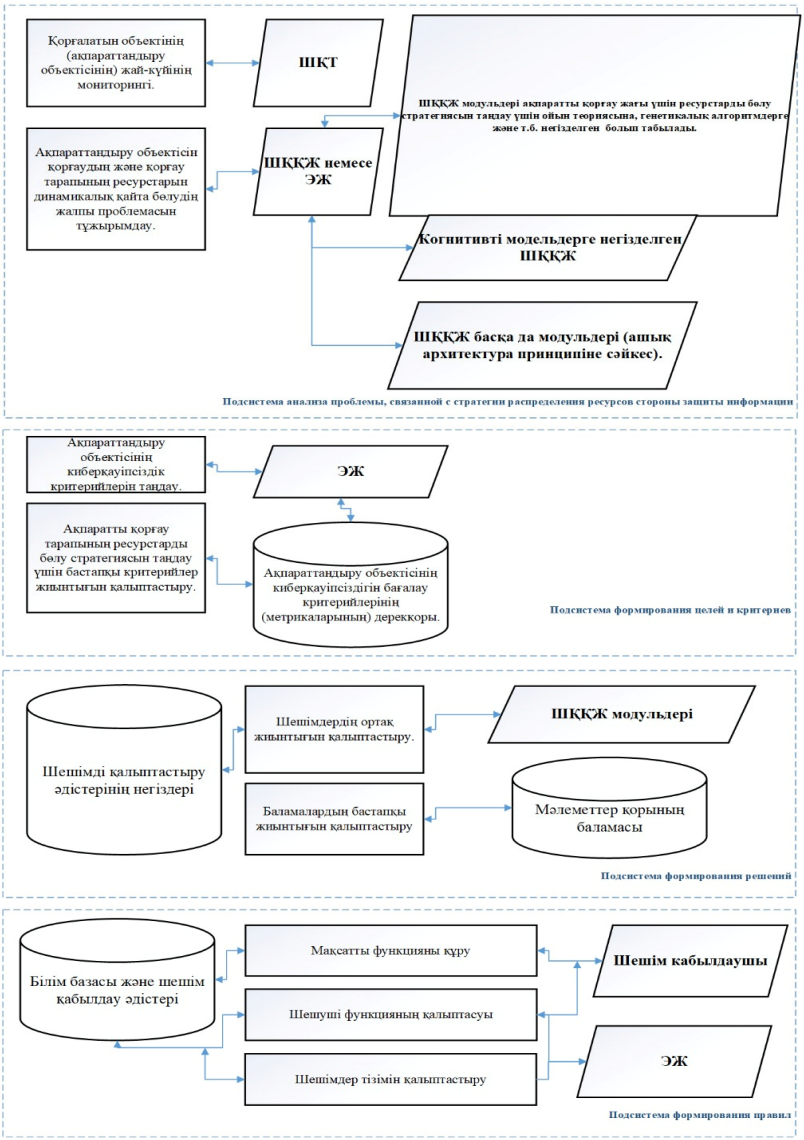
Шешім қабылдау процесінің үнемі күрделенуі, атап айтқанда басқарушылық, әртүрлі ақпараттандыру объектісі үшін кибер-қауіпсіздік қамтамасыз ету есептерін, сондай-ақ шешімдерге әсер ететін факторлардың өзара байланысын қамтитын пәндік салалардың күрделілігімен бірге шешім қабылдауды қолдау үшін сыртқы құралдарды тарту қажеттілігін анықтайды. Нашар құрылымдалған пәндік салаларда (мысалы, ақпараттық технологияларға инвестициялау, киберқауіпсіздік, атап айтқанда, ақпаратты қорғау тарабының ресурстарын серпінді қайта бөлу және т.б.), детерминистік ақпаратты шешім қабылдау үшін жеткілікті мөлшерде алу мүмкіндігі болмаған жағдайда, шешім қабылдауды сараптамалық қолдау олардың сапасын арттырудың жалғыз құралы болып табылады. Бұл, негізінен, жоғары ұйымдастырушылық деңгейлердің есептерін шешу туралы (мысалы, маңызды ақпараттандыру объектісі ақпараттық жүйелері), дұрыс емес шешімнің «бағасы» қазіргі уақытта тым жоғары және үнемі өсіп келеді. Егер әртүрлі ақпараттандыру объектісі үшін киберқауіпсіздік ресурстарын серпінді басқару есептеріндегі шешімдерді қолдау туралы айтатын болсақ, онда хакерлер тарапынан мемлекеттік және жеке компаниялардың ат инфрақұрылымына деструктивті әсердің саны мен күрделілігінің қарқынды өсуімен бірге ресурстарды бөлу стратегиясын дұрыс таңдау ақпараттық массивтердің, беделдің жоғалуына ғана емес, сонымен қатар кибершабуыл объектісін қаржыландыруға айтарлықтай зиян келтіруі мүмкін.

4.1. Ақпараттандыру объектілерінде ақпаратты қорғау тарапының ресурстарын бөлу есепі үшін ОҚҚЖ тұжырымдамалық жобалау

Нақты ақпараттандыру объектісі үшін ақпаратты қорғау тарабының ресурстарын бөлу процесінде шешімдер қабылдауды қолдау жүйесі оны кез келген мүдделі тұлғалардың барлық мекемелерде немесе кәсіпорындарда пайдалануы мақсатында құрылады, олар үшін қорғаныс жағының ресурстарды бөлудің ұтымды стратегиясын табу есепі компьютерлік зиянкестердің ақпараттық ресурстарға деструктивті әсер етуінің саны мен күрделілігінің артуы жағдайында өзекті болып табылады [97].

Шешім қабылдауды қолдау жүйесі келесі есептерді шешуге бағытталған. Білім, мәліметтер базаларын, ақпаратты қорғау тарабының ресурстарын бөлу стратегиясын таңдаумен байланысты әртүрлі жағдайларға база құру, пайдаланушылардың қолжетімділігін шектей отырып, ақпараттандыру объектісі қорғау тарабының ресурстарын серпінді бөлу стратегияларының бірыңғай электрондық мұрағатын жүргізу үшін бағдарламалық қамтамасыз етуді әзірлеу. Ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегияларын есепке алу, деректер форматтары мен алмасу хаттамаларын ішкі стандарттау есебінен шешім қабылдауды қолдау жүйесі кіші жүйелері арасындағы ақпараттық өзара іс-қимылды қамтамасыз ету саласында бірыңғай ақпараттық кеңістік құру. Ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегияларын таңдау бойынша шығыс құжаттамасын қалыптастырудың бірыңғай жүйесін құру. Шешім қабылдайтын тұлғаға қажетті құжаттардың үлгілері мен шаблондарының деректер базасын жүргізу. Шешім қабылдау үшін аналитикалық ақпаратты графикалық және баспа түрінде қалыптастыру. Ақпараттандыруды дамытудың жүйелілігін, кешенділігін және келісімділігін қамтамасыз ету, сүйемелдеу мен бақылаудың дәстүрлі нысандары мен әдістерін пайдалана отырып, ақпаратты қорғау тарабының ресурстарын бөлу есептері. Ақпараттық және кибернетикалық қауіпсіздік бағдарламалары үшін шешім қабылдауды қолдау жүйесінің негізгі функциялары,

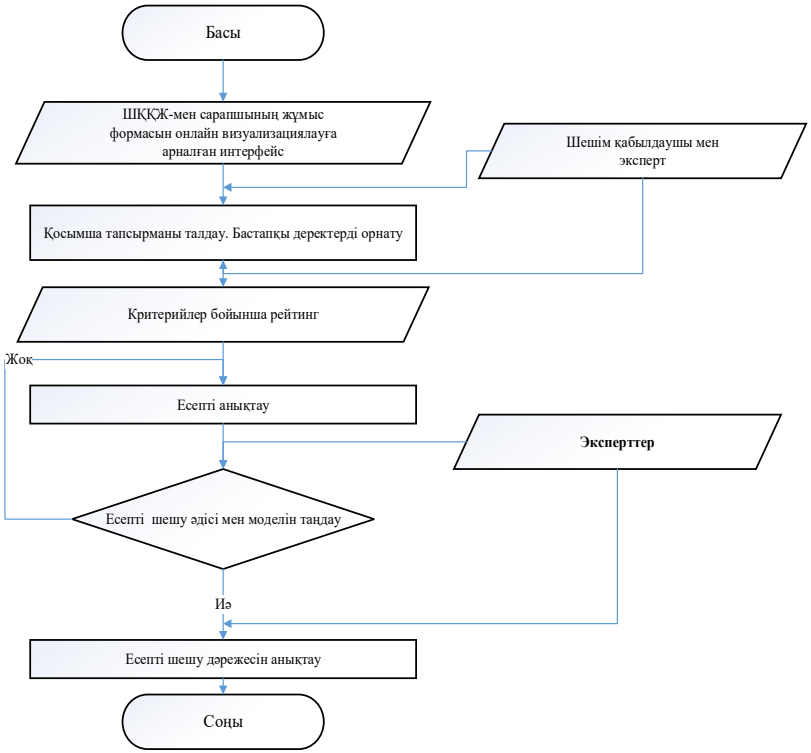
әдетте, мыналарды сақтау қажеттілігіне қарай регламенттеледі: киберқауіпсіздік проблематикасын кешенді талдау принциптері; шешімдерді қолдау процесінде қолданылатын ресми және бейресми әдістерді біріктіру мүмкіндіктері; есептің ағымдағы жағдайына қатысты ақпараттың сенімділігі мен өзектілігі принциптері. Бұл ретте, әдетте, әртүрлі есептерді, статистикалық деректерді, талдамалық шолуларды, сондай-ақ мониторингтің кіші жүйелерінен алынатын деректерді пайдаланады; шешім қабылдауды интеллектуализациялау үшін әдістер мен модельдерді автоматтандырылған таңдау принциптері; шешім қабылдауды қолдау жүйесі жағдайын одан әрі дамыту қағидаттары; шешім қабылдауды қолдау жүйесі жұмыс істеу тиімділігін және қабылданған ұсыныстар мен қорытындылардың негізділігін арттыру мақсатында шешім қабылдауды қолдау жүйесін серпінді басқару қағидаттары, оларды шешім қабылдаушы тұлғаның бақылау іс-шараларын әзірлеу процесінде пайдалана алады; талдау, жедел басқару және шешілетін тапсырманы бақылау модульдерінің әлеуеті [98]. Шешім қабылдауды қолдау жүйесі толық жұмыс істеуін қамтамасыз ету үшін әдетте бірнеше негізгі модульдер мен кіші жүйелерді қамтиды. Бұл жүйеге шешім қабылдау үшін қолданылатын мәліметтер базалары, білім базалары, модельдер мен ережелер базасы кіреді. Интерфейсті басқару жүйесі шешім қабылдауды қолдау жүйесінің архитектурасы бойынша, жергілікті немесе клиент-серверлік негізде жобаланады. Сондай-ақ, басқа модульдер мен ішкі жүйелер де болуы мүмкін, олардың қажеттілігі пәндік аймақтың ерекшелігімен байланысты. Шешім қабылдауды қолдау жүйесі шешім қабылдауды қолдаудың бірнеше түрін қамтамасыз етуі тиіс: сараптамалық қолдау, автоматтандырылған шешім шығару және аралас шешім.



4.1-сурет. Ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегиясын таңдауға қатысты шешімдер қабылдау процесіндегі шешім қабылдауды қолдау жүйесі архитектурасы.

Шешім қабылдауды қолдау жүйесі (немесе ЭЖ) өзегі білім базасы болып табылады. Осы пәндік білім базаларында ақпаратты қорғау тарабының ресурстарын серпінді бөлу есептеріндегі сарапшылардың білімі жинақталатын болады. Білімді эвристикалық ережелер форматында ұсынған жөн [99]. Білім базаларында оқыту және жаңа білім жинақтау келесідей жүзеге асырылады. Ақпаратты қорғау тарабының ресурстарын серпінді бөлудің нақты есептерін қарау кезінде оны шешуді қамтамасыз ететін ереже қалыптастырылады. Әзірленген ережелер нақты тапсырманың ерекшелігіне байланысты ережелер базасына орналастырылады. Шешім қабылдауды қолдау жүйесі ереже базасында қажетті ережені іздеуді, мысалы, семантикалық модельдер негізінде жүзеге асырады. «Ақпараттандыру объектісінің ақпараттық ресурстарын серпінді бөлу проблемалары мен тәуекелдерін талдау» ішкі жүйесінің жұмыс алгоритмі блок-схема түрінде көрсетілген. Ақпаратты қорғау тараптарының ресурстарын серпінді бөлу кезінде жиі кездесетін есептердің төрт класы бар. Біріншісі – стандартты есептер, олар шешім қабылдаушы тұлға белгілеген нұсқауларды қолдануды қажет етеді. Екіншісі – жақсы құрылымдалған есептер, олар сандық сипаттамалар мен көрсеткіштерге ие және әдетте экономикалық және математикалық әдістерді қолдану арқылы шешіледі. Үшіншісі – нашар құрылымдалған есептер, олар сандық сипаттамалармен қатар сапалық сипаттамаларға ие, мұндай есептерді шешу үшін жүйелі талдау әдістерін қолдану қажет. Төртіншісі – құрылымданбаған есептер, оларды шешу белгілі бір пән саласына сарапшылар тартуды қажет етеді. «Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлу үшін проблемалар мен тәуекелдерді талдау» кіші жүйесі есептерді одан әрі шешу мақсатында іздестіруді және тұжырымдауды қамтамасыз етуге тиіс. Осы ішкі жүйенің негізгі бағыттарына ақпаратты қорғау тарабының ресурстарын серпінді бөлу объектілерінің мониторингі, сандық критерийлер мен көрсеткіштерді айқындау, аргументтер негізінде есептер көзін анықтау, есепті тұжырымдау әдісін таңдау, жалпы есепті тұжырымдау, есептің белгісіздік дәрежесін анықтау және жалпы есеп шеңберіндегі жеке есептерді белгілеу кіреді.Есепті анықтағаннан кейін ақпараттандыру объектісінің ақпаратын қорғау тарапының ресурстарын серпінді бөлуді іске асыру тиімділігінің мақсаттар тізбесін

және критерийтар жүйесін қалыптастыру қажет. Бұл есепті кейіннен бағалау және оны одан әрі шешу жолдарын табу үшін қажет. Ол үшін шешім қабылдауды қолдау жүйесінде «ақпараттандыру объектісі ақпаратын қорғау тарабының ресурстарын серпінді бөлу стратегиясын бағалау үшін мақсаттар мен өлшемдер жүйесін қалыптастыру» деген жеке кіші жүйе бар, 4.3-суретті қараңыз. Ақпараттандыру объектісі ақпаратын қорғау тараптарының ресурстарын серпінді бөлу кезінде қол жеткізуге болатын мақсатты немесе көптеген мақсаттарды қалыптастыру кезінде әртүрлі есептер туындауы мүмкін. Бұл есептер біріктірілуі; бір-біріне қайшы келуі; өзара ерекше болуы және т. б. мүмкін.

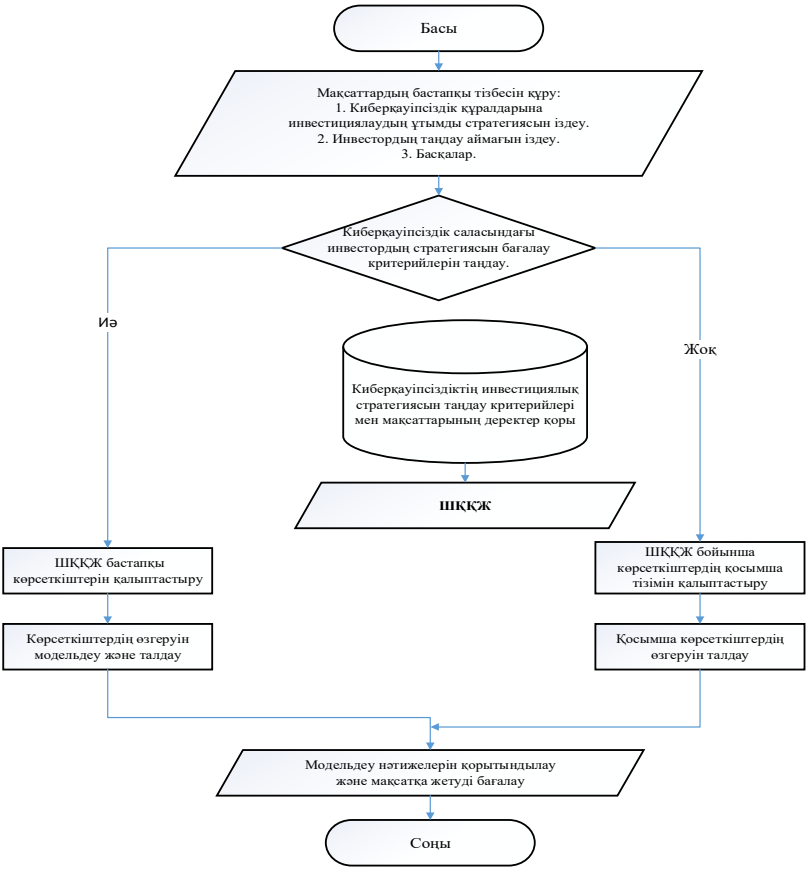


4.2-сурет. «Ақпараттандыру объектісі ақпаратын қорғау тарабының ресурстарын серпінді бөлу есепі үшін проблемалар мен тәуекелдерді талдау» кіші жүйесінің жұмыс істеу алгоритмінің блок-схемасы

Ақпараттандыру объектісі ақпаратын қорғау тараптарының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу, тиімділікті бағалау критерийлерінің мақсаттары мен жүйесін қалыптастыру сияқты күрделі проблематиканы: сарапшылар тұжырымдайтын қағидатты жаңа новаторлық мақсаттарға; ұқсас жағдайларда туындаған мақсаттарға ұқсас типтік мақсаттарға; нақты шешім қабылдауды қолдау жүйесі үшін генерациясы қолжетімді құрамдастырылған мақсаттарға бөлген жөн [100].

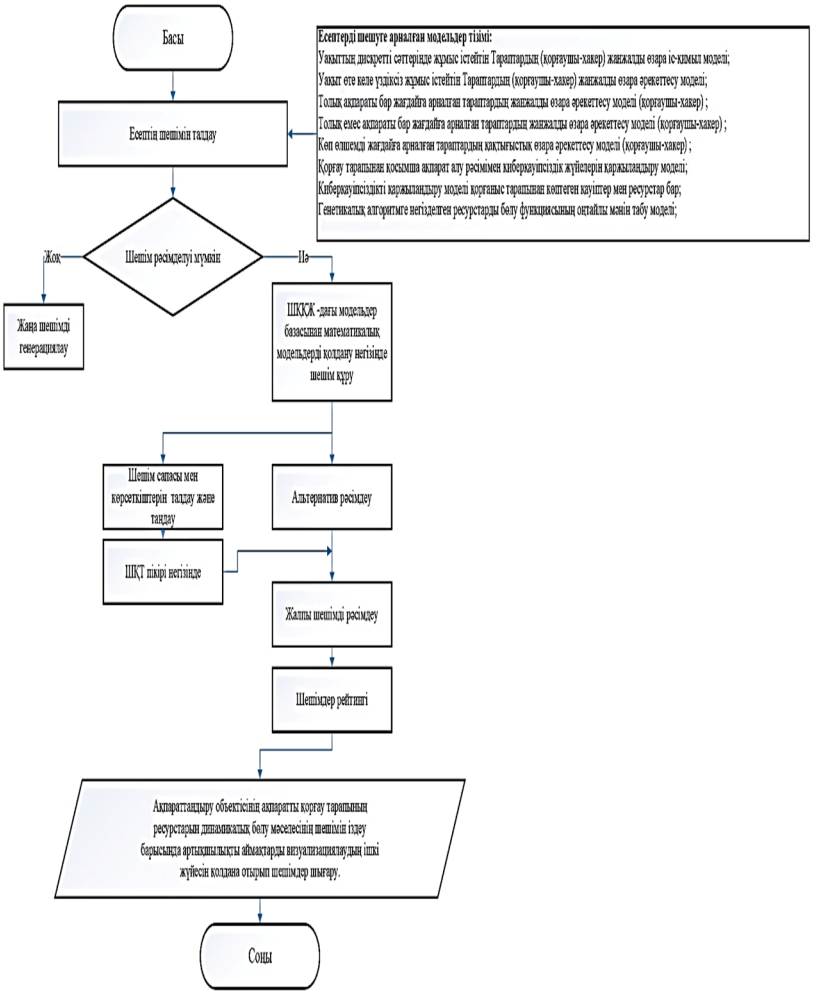
Мақсаттар мен тиімділік критерийлерін қалыптастырудың ең тиімді әдісі сарапшылармен өзара әрекеттесетін бағдарламалық жүйелер болып табылады. «Ақпараттандыру объектісі ақпараттарын қорғау тарабының ресурстарын серпінді бөлу стратегиясын бағалау үшін мақсаттар мен өлшемдер жүйесін қалыптастыру» кіші жүйесі шешім қабылдауды қолдау жүйесінің одан әрі жұмыс істеуі үшін мақсаттар мен критерийтар жүйесін кезең-кезеңімен қалыптастыруды қамтамасыз етуі тиіс. Сонымен қатар, бұл ішкі жүйеде ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлу тиімділігінің критерийлері мен көрсеткіштерінің көп деңгейлі иерархиясы іске асырылған. Қосалқы мақсаттар үшін критерийларды декомпозициялау мүмкіндігі қамтамасыз етілген. Сондай-ақ, ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлу тиімділігінің критерийлері мен көрсеткіштері арасындағы математикалық тәуелділіктерді анықтау мүмкіндіктері қарастырылған. Шешім қабылдауды қолдау жүйесі ұсынған стратегияны көрнекі бағалау үшін шкалаларды, өлшем бірліктерін және маркерлерді таңдау мүмкіндігі де енгізілген. Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлудің ұтымды стратегиясын таңдау есебін одан әрі талдау үшін шешімдердің баламалы нұсқаларын қалыптастыру қажет. Бұл баламалы нұсқалар «Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлу процесінде қабылданатын шешімдерді қалыптастыру» кіші жүйесінде қалыптастырылады. «Шешімдерді қалыптастыру» ішкі жүйесінің жұмыс алгоритмінің блок-схемасы 4.4-суретте көрсетілген. Ақпараттандыру объектісі қорғаныс жағының ресурстарын серпінді бөлудің ұтымды стратегияларын іздеу есептеріне арналған мүмкін шешімдерді қалыптастыру қазіргі уақытта ойын теориясының немесе серпінді бағдарлама-

лаудың математикалық аппаратын қолдану негізінде жүзеге асырылады. Ақпараттандыру объектісі қорғау жағының ресурстарды серпінді бөлудің ұтымды стратегиясын таңдау: жоғарыда 2 және 3-тарауларда ұсынылған аналитикалық модельдерді бағдарламалық қамтамасыздандыру арқылы жүзеге асырылады. Бұл жүйелердің сараптамалық кіші жүйелерін пайдалану арқылы; шешім қабылдаушы тұлға берген немесе шешім қабылдауды қолдау жүйесі білім базасынан алынған түрлі модельдердің комбинациясы арқылы сценарийлер құру арқылы орындалды.



4.3-сурет. Кіші жүйенің жұмыс істеу алгоритмінің блок-схемасы

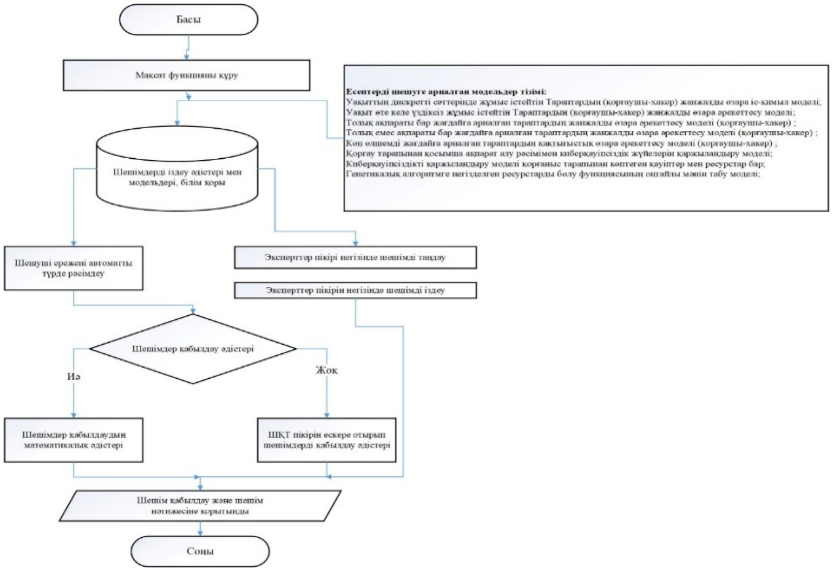
«Ақпараттандыру объектісінің ақпаратын қорғау тарабының ресурстарын серпінді бөлу стратегиясын бағалау үшін мақсаттар мен критерийтар жүйесін қалыптастыру»



4.4-сурет. Ақпараттандыру объектісі қорғау тарабының ресурстарын серпінді бөлу процесінде қабылданатын шешімдерді қалыптастыру кіші жүйесінің жұмыс істеу алгоритмінің блок-схемасы

Шешімдерді қалыптастыру процесі екі түрге бөлінеді. Біріншісі – әзірге шешім қабылдауды қолдау жүйесі әзірлемейтін жаңашыл шешімдер, мысалы, білім базасында әзірге үлгі жоқ жағдайлар. Екіншісі – типтік сценарийлерге негізделген шешімдер, яғни белгілі шешімдермен аналогия қолданылатын нұсқалар. «Ақпараттандыру объектісі қорғау тарабының ресурстарын серпінді бөлу процесінде қабылданатын шешімдерді қалыптастыру» кіші жүйесі көптеген шешімдерді қалыптастыруды мынадай жүйелілікке сәйкес қамтамасыз етеді: математикалық модельдер немесе сараптамалық әдістерді пайдалана отырып шешімдер жиынын генерациялау, балама шешімдерді құрылымдау, және баламаларды талдау кезеңінде одан әрі өңдеу арқылы үздік шешімдерді таңдау үшін баламалы шешімдердің түпкілікті жиынтығын қалыптастыру. «Ақпараттандыру объектісі қорғаныс жағының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» ішкі жүйесі функционалдық әрекеттердің келесі тізбегін ұсынады. Есептің шарттары бойынша шешімді таңдау үшін шешуші ереже қалыптастырылады. Бұл процесс автоматтандырылған режимде немесе сарапшылар тобын тарта отырып жүргізіледі. Соңғы жағдайда сарапшылар бұрын құрылған критерийлер жүйесі үшін шешілетін есепке байланысты шешуші функцияны қалыптастырады. Шешуші ережені қалыптастырудың негізі – критерийлердің иерархиялық құрылымдары үшін көп критерийлі артықшылық функциясы. Сонымен қатар, шешуші ереже ақпараттандыру объектісі қорғаныс жағының ресурстарын серпінді бөлудің ұтымды стратегиясын таңдауға ықпал ететін математикалық және эвристикалық ережелерді де қамтиды. Қалыптасқан шешуші функция негізінде неғұрлым тиімді шешім таңдалады. Ақпараттандыру объектісін қорғау тарабының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу барысында баламаларды талдау және таңдау қалыптасқан шешуші ереже бойынша жүзеге асырылады. Шешім болмаған жағдайда ішкі жүйеде шешім нұсқаларына сараптамалық бағалау жүргізу мүмкіндігі қарастырылған, оны ақпараттандыру объектісі киберқауіпсіздікті қамтамасыз етудің есептік-бағдарланған саласына сарапшыларды тарту арқылы жүзеге асыруға болады. Шешуші ережені қалыптастыру ақпараттандыру объектісін қорғау тарабының ресурстарын серпінді бөлу

стратегиясын бағалау барысында туындайтын түрлі жағдайларға байланысты қалыптасқан білім базалары, ережелер базасы негізінде сараптамалық жүйемен бірлесіп жүзеге асырылады. Мақсатты функцияны сараптамалық қалыптастыру сарапшылар мен шешім қабылдауды қолдау жүйесінің өзара іс-қимылын ұйымдастыру арқылы олардың пікірлерін білім базаларына енгізу негізінде іске асырылады.



4.5-сурет. «АОБ қорғау тарабының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» кіші жүйесінің блок-схемасы

«Ақпараттандыру объектісі қорғау жағының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу барысында шешуші ережені қалыптастыру және баламаларды талдау» ішкі жүйесі шешуші функцияны автоматтандырылған режимде де, сараптамалық пікірлерді есепке алу негізінде де құруға мүмкіндік береді. Ережелерді тәуелсіз қолдану бастапқы шешімдерді және олардың осы ішкі жүйенің жұмыс істеуі нәтижесінде алынған шешімдерді салыстыруға мүмкіндік береді. Шешім қабылдауды қолдау жүйесі сараптамалық кіші жүйесі жасанды интеллекттің негізгі қосым-

шаларының бірі болып табылады және білім базаларында сақталатын нақты пәндік салаға қатысты есептерді шешуге арналған.

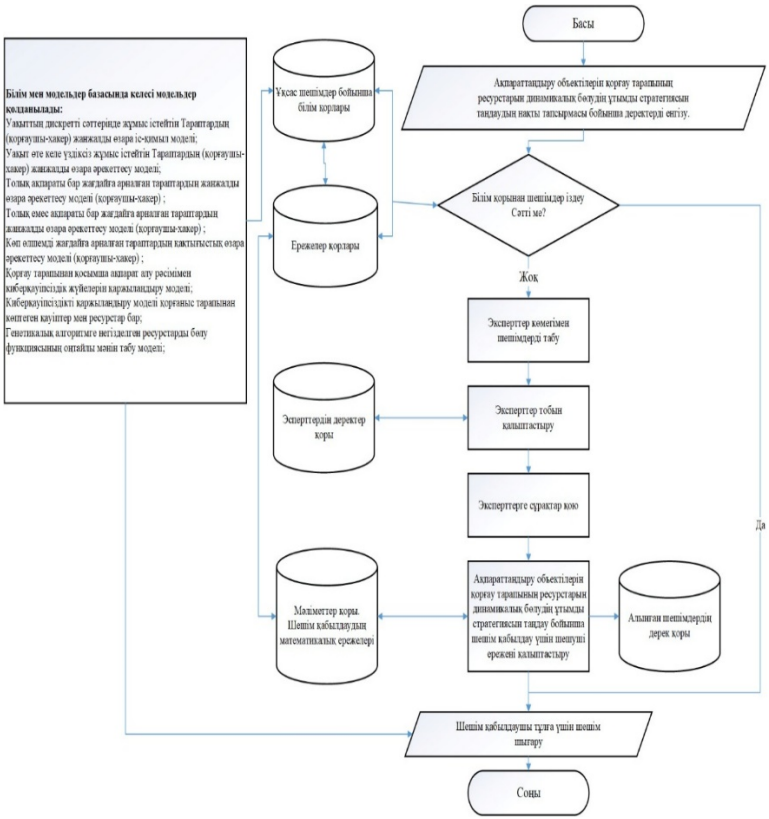
Ақпараттандыру объектісі қорғау тарабының ресурстарын серпінді бөлудің ұтымды стратегиясын іздеу үшін шешім қабылдауды қолдау жүйесі негізі ретінде сараптамалық кіші жүйенің негізгі мақсаты бұрын [87 164-170-б., 91, 469-470-б.] сипатталған модельдер негізінде әртүрлі есептерді шешуге бағдарлау болып табылады.Сараптамалық ішкі жүйенің жұмыс істеу алгоритмінің блок-схемасы 4.6-суретте көрсетілген.

Сараптамалық ішкі жүйе сарапшы мамандардан алынған білім есебінен пайдаланушының ақпараттандыру объектісін қорғау тарабының ресурстарын серпінді бөлу стратегиясының ықтимал баламаларын әзірлеуді және бағалауды қамтамасыз етеді. Сараптамалық ішкі жүйе мыналардан тұрады:Есепті шешу барысында жинақталған бастапқы және аралық фактілерді сақтауға арналған білім базалары. Сондай-ақ, модельдер мен модельдерді басқару ережелері білім базаларында сақталады. Сондай-ақ, егер ақпараттандыру объектісі қорғаныс жағының ресурстарын серпінді бөлудің ұтымды стратегиясын таңдау есебін шешу барысында қолданылатын ережелер көп болса, ережелердің жеке базасын жобалауға болады; Ақпараттандыру объектісі қорғау жағының ресурстарын серпінді бөлудің ұтымды стратегиясын таңдаумен байланысты есептерді шешу блогы. Бұл блок мәлімет базалары және білім базаларында сақталатын өлшемдер мен қағидалар негізінде ақпараттандыру объектісін қорғау тарабының ресурстарын серпінді бөлудің нақты есепін шешу үшін ережелерді орындау кезектілігінің іске асырылуын қамтамасыз етеді; Шешім қабылдауды қолдау жүйесі ұсынатын шешім қабылдаушы тұлға мұндай шешімнің себебін түсінуге мүмкіндік беретін түсініктеменің ішкі жүйесі; Білім базаларына жаңа ережелер қосуға және/немесе оларды өзгертуге арналған ережелерді қалыптастыру модулі;

Жалпы алғанда, пайдаланушының ішкі жүйемен және шешім қабылдауды қолдау жүйесімен ыңғайлы диалогын жүзеге асыруға арналған диалогтық интерфейс.4.6-суретте көрсетілген алгоритмнің жұмыс істеу әрекеттерінің реттілігі келесідей.

Тапсырмалар туралы ақпарат алған кезде шешім қолданыстағы білім базаларында ізделеді. Егер осыған ұқсас жағдай бұрын

кездесіп, шешім қабылдау ережелері анықталса, онда шешім осы есеп бойынша нақты анықталады.



4.6-сурет. Жобаланатын шешім қабылдауды қолдау жүйесі үшін сараптамалық кіші жүйенің жұмыс істеу алгоритмінің блок-схемасы

Егер есепті бастапқы қоюға шешім болмаса, онда есеплік-бағытталған сарапшылар тобы құрылады. Әрі қарай сарапшыларға жаңа шешуші ережені қалыптастыруға көмектесетін сұрақтар жіберіледі. Сарапшылар ең жақсы балама және тиісті шешім қабылдауды қолдау жүйесі ішкі жүйесін таңдау үшін шешуші ереже қалыптастырады. Келесі кезеңде ең жақсы шешімді таңдау анықталады. Шешім есептің бастапқы тұжырымына сәйкес кел-

ген жағдайда ереже ережелер базасында, ал шешім білім базаларына жазылады. Шешім қабылдауды қолдау жүйесі жұмыс істеуінің осы алгоритмі ақпараттандыру объектісі қорғау тарабының ресурстарын серпінді бөлу стратегиясын таңдаумен байланысты кез келген есеп үшін талдау және шешімді табу мүмкіндігін қамтамасыз етеді.

4.2. Ақпараттандыру объектісін қорғау тарабының ресурстарын серпінді бөлудің ұтымды стратегияларын іздеу барысында шешім қабылдауды қолдау жүйесі модульдерін бағдарламалық іске асыру

Әзірлеген «Decision support systems dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі бірнеше кіші жүйелерден тұрады. Жоғарыда көрсетілгендей, жаңа модульдерді шешім қабылдауды қолдау жүйесі өзегіне қосудың орындылығына байланысты оның архитектурасы модульдік принцип бойынша құрылған. Мұндай «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі архитектурасы оны айтарлықтай икемді іске асыруға мүмкіндік береді, мысалы, жаңа модульдерді жазу шамасына қарай қолданыстағы модульдердің функционалына әсер етпей, оларды бас модульге қосуға болады. Осылайша, пайдаланушы тарапта (ақпараттандыру объектісі үшін ақпаратты қорғау тарабы) қажет болған жағдайда шешім қабылдауды қолдау жүйесі бастапқы архитектурасын жаңа функционалдық модульдермен толықтыруға мүмкіндік бар. «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі бағдарламалық іске асыру қосымшаның MDI стилінде орындалған, 4.7-суретті қараңыз. Осылайша, сарапшылар бір уақытта барлық «Decision support systems Dynamic allocation of cyber security resources» модульдерімен жұмыс істей алады.

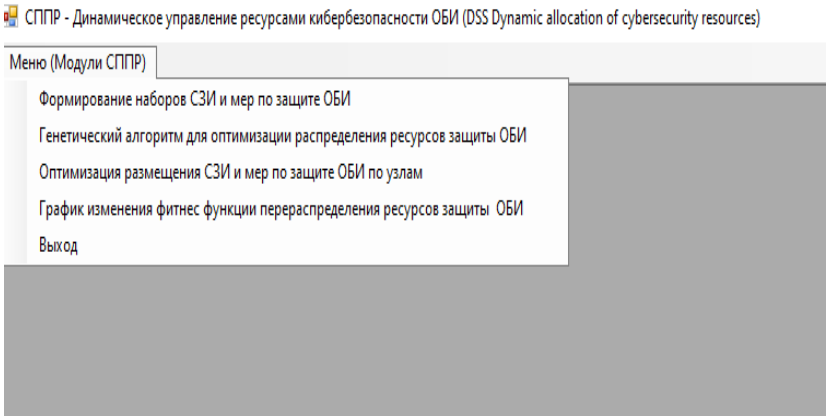
Файл мәзірінің тармағында монографиялық зерттеу барысында іске асырылған шешім қабылдауды қолдау жүйесі модульдері келтірілген. Қазіргі кезде бағдарламалық түрде [92] мынадай шешім қабылдауды қолдау жүйесі модульдері іске асырылды:

1-модуль – ақпараттандыру объектісі үшін ақпаратты қорғау құралдары жинақтарын және қорғау әдістерін қалыптастыру;

2-модуль – ақпараттандыру объектісі қорғау ресурстарын бөлуді оңтайландыруға арналған генетикалық алгоритм (монографияның 2-1 және 3-тарауларында ұсынылған модельдер негізінде);

3-модуль – ақпаратты қорғау құралдарын орналастыруды және түйіндер бойынша ақпараттандыру объектісі қорғау жөніндегі шараларды оңтайландыру (монографияның 2-тарауында ұсынылған модельдер негізінде);

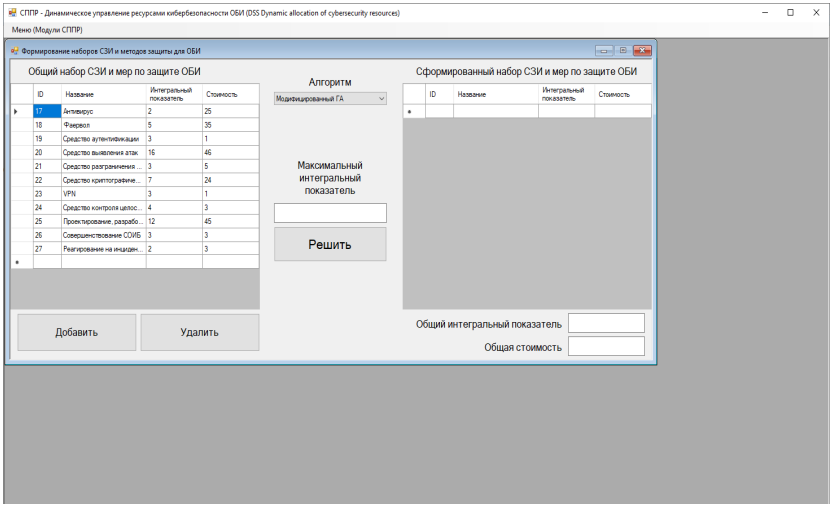
4-модуль – ақпараттандыру объектісі қорғаныс ресурстарын қайта бөлу функциясын өзгерту кестесі.



4.7-сурет. «Decision support systems Dynamic allocation of cyber security resources» негізгі терезесінің жалпы көрінісі

Бұл модульдердің мақсаты мен сипаттамасы төменде келтірілген. «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі сарапшысының жұмысы «ақпараттандыру объектісі үшін ақпаратты қорғау құралдары жиынтығы мен қорғау әдістерін қалыптастыру» бірінші модулінен басталады. Бұл модуль интерфейсінің жалпы көрінісі төменде 4.8-суретте көрсетілген. Сол жақта мәліметтер базасынан деректерді визуализациялау интерфейсі көрсетілген (Accessilimssqlserver), онда белгілі бір ақпараттандыру объектісінің ерекшелігіне сүйене отырып, ақпаратты қорғау құралдары мен шараларының нұсқалары бар. Әрбір ақпараттандыру объектісі үшін негізгі шаралар мен

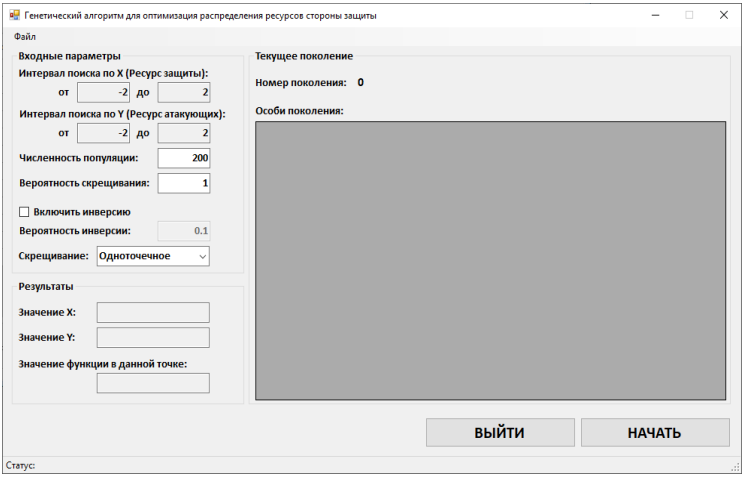
құралдар кәсіпорындағы ақпараттық массивтердің құнына байланысты ерекшеленуі мүмкін. Оң жақта ұсынылған шаралар мен ақпаратты қорғау құралдарын таңдау нәтижелері бар интерфейс көрсетілген. Бұл жағдайда екі алгоритмді таңдауға болады: қарапайым сұрыптау (i7 процессоры үшін шамамен 30 минут уақыт қажет) немесе модификацияланған генетикалық алгоритм (жұмсалған уақыт i7 процессоры үшін 1 минуттан аспады).



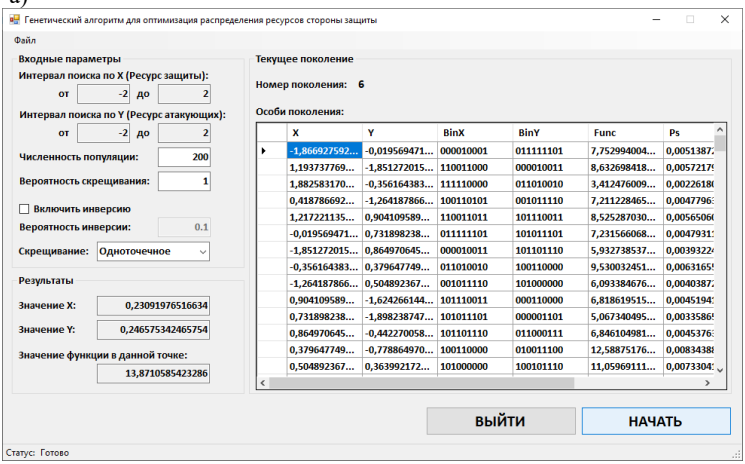
4.8-сурет. Модульдің жалпы көрінісі 1 – ақпараттандыру объектісі үшін ақпаратты қорғау құралдары жиынтығы мен қорғау әдістерін қалыптастыру

Әрі қарай, 2-модульді (4.9-суретті қараңыз) – ақпараттандыру объектісі қорғау ресурстарын бөлуді оңтайландырудың генетикалық алгоритмін пайдалана отырып, қауіптерді жүзеге асыру нәтижесінде келтірілген залалды және ақпараттандыру объектісі нысандарында ақпараттық ресурстарының осалдығын сипаттайтын модельдің мақсатты функциясын зерттеуге болады. Функцияның толық сипаттамасы жұмыстың екінші тарауында берілген.

4.9-суретте а) 2 модуль интерфейсінің жалпы көрінісі көрсетілген.



а)



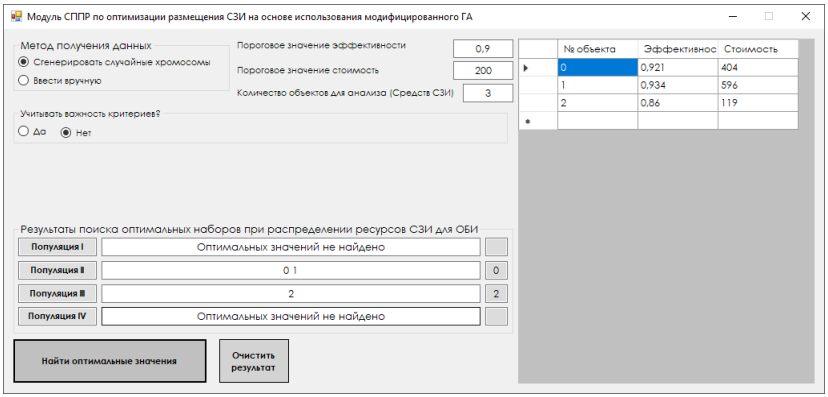
б)

4.9-сурет. 2 модульдің жалпы түрі – ақпараттандыру объектісі қорғау ресурстарын бөлуді оңтайландыруға арналған генетикалық алгоритм

4.9 б) суретте мақсатты функцияға кіретін және ақпараттандыру объектісінде ақпаратты қорғауды қамтамасыз ету жөніндегі жұмыстар тізбесіне тәуелді ұтымды параметрлерді (бұл параметрлер ақпараттандыру объектісі үшін ақпаратты қорғау құралдарына арналған шығындардың өнімділігіне сәйкес келеді немесе жалпы жағдайда нақты ақпаратты қорғау құралдарының тиім-

ділік көрсеткіштері мен оларды сатып алуға, қызмет көрсетуге, жаңғыртуға арналған шығындар көрсеткіштерінің арақатынасы) іздеу есебін шешудің мысалы көрсетілген (атап айтқанда, кешенді ақпаратты қорғау құралдары жобалау, әзірлеу және өрістету, ақпараттық қауіпсіздік (ақпараттық қауіпсіздікті қамтамасыз ету жүйесі) қамтамасыз ету жүйесін жетілдіру және т. б.). Модификацияланған генетикалық алгоритмде қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді оңтайландырудың көп критерийлі есепін шешу үшін Беллман-Заде қағидаты қолданылды. Бұл ақпараттандыру объектісі құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді оңтайландыруға және шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда ақпараттандыру объектісі қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік берді. Әрі қарай, сарапшы 3-модульді – ақпаратты қорғау құралдары орналастыруды оңтайландыру және түйіндер бойынша ақпараттандыру объектісі қорғау шаралары – іске қосуы керек.

3-модульдің жалпы көрінісі 4.10-суретте көрсетілген.



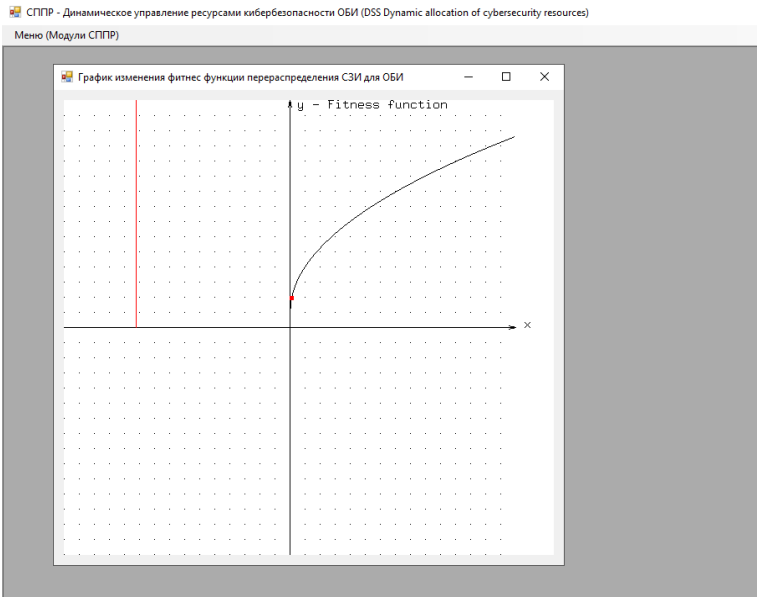
4.10-сурет. 3-модульдің жалпы түрі – түйіндерде ақпараттандыру объектісін қорғау бойынша ақпаратты қорғау құралдарын орналастыруды оңтайландыру

3-модульде ақпараттандыру объектісі ақпараттық-коммуникациялық жүйелерінің қауіпсіздік контурлары үшін ақпаратты қорғау құралдары конфигурацияларының нұсқаларын іріктеумен және оңтайландырумен байланысты есепті шешу үшін Генетикалық алгоритм модификациясы бағдарламалық түрде іске асырылған. Модификацияланған генетикалық алгоритмде (жұмыстың 3-тарауында сипатталған) ақпаратты қорғау құралдары құрамын оңтайландыру үшін критерийтар ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасы, ақпаратты қорғау құралдарының интегралдық көрсеткіштері, сондай-ақ ақпаратты қорғау құралдарының әрбір класы үшін құндық көрсеткіштері пайдаланылды. 2 және 3 модульдерде ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдары құрамын таңдауды оңтайландыру есебінде модификацияланған генетикалық алгоритм көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл жағдайда белгілі бір ақпараттандыру объектісі үшін ақпараттық-коммуникациялық жүйе қорғаныс контурлары бойынша ақпаратты қорғау құралдары орналастыруды оңтайландыру рюкзактың комбинаторлық есепін өзгерту ретінде қарастырылады. Ұсынылған тәсіл ақпараттық-коммуникациялық жүйе түйіндерінің әрқайсысы үшін ақпаратты қорғау құралдары жиынтығын оңтайландыру жөніндегі көп критерийлі-есепті шешуге ғана емес, сонымен қатар ақпараттандыру объектісі киберқауіпсіздік бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарабының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді.

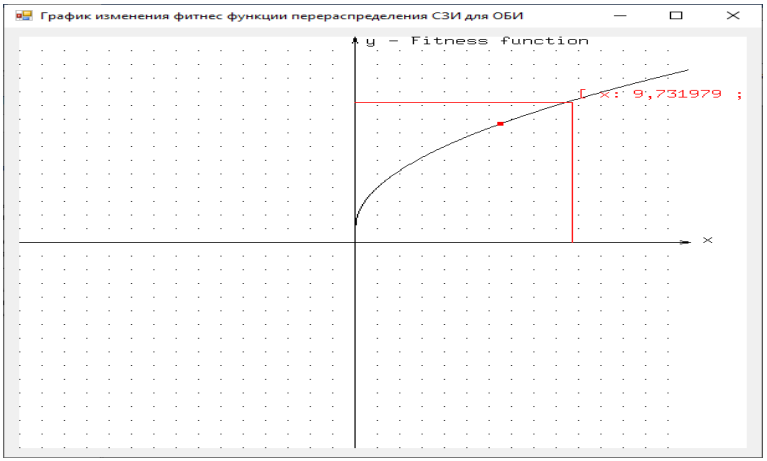
4.11 А) және б) суреттерде 4-модуль жұмысының мысалдары көрсетілген - ақпараттандыру объектісі қорғаныс ресурстарын қайта бөлу функциясының фитнес өзгеру кестесі.Графиктердегі қызыл нүктенің қозғалысы генетикалық алгоритм кезінде ұрпақтардың итерациясының өзгеруін көрсетеді. Уақыт шкаласы шартты бірліктерде ұсынылған (мысалы, минут немесе он минут, өйткені әртүрлі процессорлары бар компьютерді қолданған кезде есепті шешу уақыты дұрыс болмауы мүмкін).«Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды

қолдау жүйесі тестілеу барысында ақпараттандыру объектілерінің ақпараттық-коммуникациялық жүйе үшін киберқауіпсіздік құралдарын орналастырудың ұтымды нұсқаларын таңдау бойынша есептеу эксперименттері орындалды («Спецавтоматика в приложении» ЖШҚ үшін енгізу туралы акт). Бұл, атап айтқанда, шектеулі жағдайларда қорғаныс ресурстарын қайта бөлу есебін шешу үшін қажет. Осы «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі қолдану аппараттық-бағдарламалық ақпаратты қорғау құралдары және олардың ақпараттық-коммуникациялық жүйеге арналған комбинацияларының әртүрлі нұсқаларын жылдам сұрыптауды орындауға ғана емес, сонымен бірге олардың ерекшелігіне қарай, ақпараттандыру объектісі үшін ақпараттық-коммуникациялық жүйе киберқауіпсіздік контурларының құрамын оңтайландыру бойынша қолда бар модельдермен және алгоритмдермен келтірілген модельдер мен алгоритмдерді біріктіруге мүмкіндік береді. Модельдер мен алгоритмдердің мұндай бірігуі ақпараттық-коммуникациялық жүйе қорғанысын тез қалпына келтіруге мүмкіндік береді.

Сондай-ақ, монографияның 4-тарауында өткізілген «Decision support systems Dynamic allocation of cyber security resources» - мүмкіндіктерінің практикалық құндылығы ақпаратты жоғалтудан, ақпаратты қорғау құралдары көрсеткіштері, сондай-ақ ақпаратты қорғау құралдарының әрбір класы үшін құндық көрсеткіштерден туындайтын тәуекелдердің жиынтық шамасын ескере отырып, ұсынылған генетикалық алгоритм негізінде шешім қабылдауды қолдау жүйесі үшін есептеуіш ядро үшін шешім қабылдауды қолдау жүйесі функционалының кеңеюіне қарай оның архитектурасына серпінді қосылатын кітапханаларды қосу мүмкіндігімен ашық көп модульді шешім қабылдауды қолдау жүйесі архитектурасын бағдарламалық іске асырудың нәтижелілігін растады.

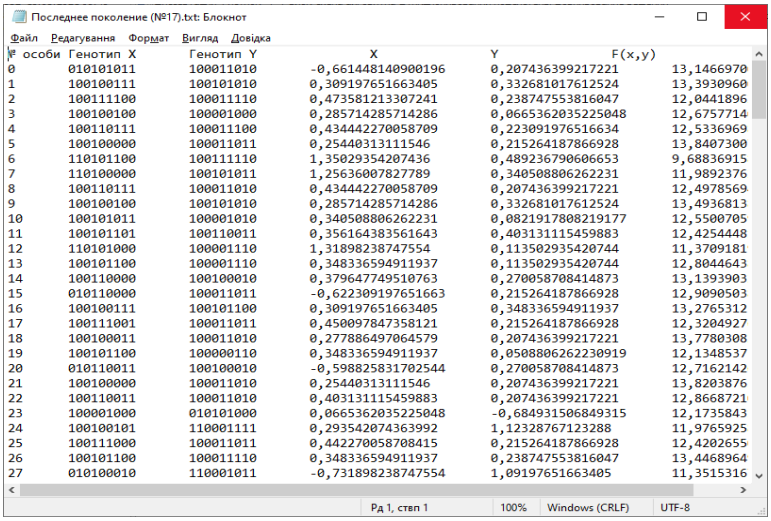


а)



б)

4.11-сурет. 4 модульдің жалпы көрінісі – ақпараттандыру объектісі қорғау ресурстарын қайта бөлу фитнес функциясын өзгерту кестесі



Последнее поколение (№17).txt: Блокнот

Файл Редагування Формат Вигляд Довідка

№ особи	Генотип X	Генотип Y	X	Y	F(x,y)
0	010101011	100011010	-0,661448140900196	0,207436399217221	13,1466970
1	100100111	100101010	0,309197651663405	0,332681017612524	13,3930960
2	100111100	100011110	0,473581213307241	0,238747553816047	12,0441896
3	100100100	100001000	0,285714285714286	0,0665362035225048	12,6757714
4	100110111	100011100	0,434442270058709	0,223091976516634	12,5336969
5	100100000	100011011	0,25440313111546	0,215264187866928	13,8407300
6	110101100	100111110	1,35029354207436	0,489236790606653	9,68836915
7	110100000	100101011	1,25636007827789	0,340508806262231	11,9892376
8	100110111	100011010	0,434442270058709	0,207436399217221	12,4978569
9	100100100	100101010	0,285714285714286	0,332681017612524	13,4936813
10	100101011	100001010	0,340508806262231	0,0821917808219177	12,5500705
11	100101101	100110011	0,356164383561643	0,403131115459883	12,4254448
12	110101000	100001110	1,31898238747554	0,113502935420744	11,3709181
13	100101100	100001110	0,348336594911937	0,113502935420744	12,8044643
14	100110000	100100010	0,379647749510763	0,270058708414873	13,1393903
15	010110000	100011011	-0,622309197651663	0,215264187866928	12,9090503
16	100100111	100101100	0,309197651663405	0,348336594911937	13,2765312
17	100111001	100011011	0,450097847358121	0,215264187866928	12,3204927
18	100100011	100011010	0,277886497064579	0,207436399217221	13,7780308
19	100101100	100000110	0,348336594911937	0,0508806262230919	12,1348537
20	010110011	100100010	-0,598825831702544	0,270058708414873	12,7162142
21	100100000	100011010	0,25440313111546	0,207436399217221	13,8203876
22	100110011	100011010	0,403131115459883	0,207436399217221	12,8668721
23	100001000	010101000	0,0665362035225048	-0,684931506849315	12,1735843
24	100100101	110001111	0,293542074363992	1,12328767123288	11,9765925
25	100111000	100011011	0,442270058708415	0,215264187866928	12,4202655
26	100101100	100011110	0,348336594911937	0,238747553816047	13,4468964
27	010100010	110001011	-0,731898238747554	1,09197651663405	11,3515316

Рд 1, ствп 1 | 100% | Windows (CRLF) | UTF-8

4.12-сурет. Шешім қабылдауды қолдау жүйесі мақсатты функциясы нәтижелерін шығарудың мысалы

Тарау шеңберінде жүргізілген есептеу эксперименттері шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда ақпараттандыру объектісін қорғау тарапының ресурстарын бөлуді оңтайландыруға мүмкіндік берді. «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі модулін бағдарламалық іске асыру кодтарының негізгі фрагменттері қосымшада келтірілген.

4.3. 4-тарау бойынша қорытындылар

Монографияның соңғы тарауында келесі негізгі нәтижелер алынды:

қарсы әрекет етуші тараппен (хакермен) серпінді қарсы тұру жағдайында ақпараттандыру объектілерінде ақпаратты қорғау тарапының ресурстарын бөлу стратегиясының ұтымды (оңтайлы) нұсқасын талдау және таңдау процесінде шешім қабылдауды қолдау жүйесі жұмыс істеуінің құрылымдық схемасы ұсынылды; Жүйенің үздіксіз және тиімді жұмыс істеуін қамтамасыз етуге ықпал ететін мұндай шешім қабылдауды қолдау жүйесінің негізгі

функционалдық модульдері қарастырылды. Осы шешім қабылдауды қолдау жүйесі мынадай негізгі кіші жүйелеріне арналған егжей-тегжейлі блок-схемалар келтірілген: есепті, тәуекелдер мен қатерлерді талдаудың кіші жүйесі, қарсы іс-қимыл жасайтын тараппен (хакермен) серпінді қарсы тұру жағдайында ақпараттандыру объектісінде ақпаратты қорғау тарабының ресурстарын бөлудің болмауына байланысты; ақпараттандыру объектісін қорғау ресурстарын қайта бөлу нәтижелілігін бағалаудың мақсаттары мен критерийлерін қалыптастырудың кіші жүйесі; шешімдерді қалыптастырудың кіші жүйесі; қарсы әрекет ететін тараппен серпінді қарсы тұру жағдайында ақпараттандыру объектісінде ақпаратты қорғау тарабының ресурстарын бөлудің шешуші ережесін қалыптастыру және балама стратегияларын талдаудың кіші жүйесі;Келтірілген схема шағын компаниялардан немесе кәсіпорындардан бастап ірі ақпараттандыру объектісіне дейінгі кез келген ауқымдағы ақпараттандыру объектісі үшін қарсы әрекет етуші тараппен (хакермен) серпінді қарсы тұру жағдайында ақпараттандыру объектілерінде ақпаратты қорғау тарабының ресурстарын бөлудің ұтымды стратегияларын таңдау процесінде шешімдердің толық функционалды қабылдануын қамтамасыз ететіндігі көрсетілген; Бірнеше ішкі жүйелерден тұратын «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі әзірленді. «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі архитектурасы модульдік принцип бойынша құрылған және бұл оны жеткілікті икемді іске асыруға мүмкіндік береді. Жаңа модульдер әзірленетіндіктен, оларды бар модульдердің функционалдық мүмкіндіктеріне әсер етпестен негізгі модульге қосуға болады. «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі бағдарламалық іске асыруы MDI қосымшалар стилінде орындалған; Пайдаланушы тараптың (ақпараттандыру объектісі үшін ақпаратты қорғау тарабы) қажет болған жағдайда бастапқы шешім қабылдауды қолдау жүйесі архитектураны жаңа функционалдық модульдермен толықтыруға мүмкіндігі бар екені көрсетілген; бағдарламалық түрде (VisualStudio 2019 бағдарламалау ортасы, бағдарламалау тілі#) мынадай шешім қабылдауды қолдау жүйесі модульдері іске асырылды: 1 модуль – ақпараттандыру объектісі

үшін ақпаратты қорғау құралдары жиынтығы мен қорғау әдістерін қалыптастыру; 2 модуль – ақпараттандыру объектісі қорғау ресурстарын бөлуді оңтайландыруға арналған генетикалық алгоритм (монографияның 2-ші және 3-ші тарауларында ұсынылған модельдер негізінде); 3 модуль – тораптар бойынша ақпаратты қорғау құралдары орналастыру мен ақпараттандыру объектісі қорғау жөніндегі шараларды оңтайландыру (монографияның 2-тарауында ұсынылған модельдер негізінде); 4 модуль – ақпараттандыру объектісі қорғау ресурстарын қайта бөлу функциясының фитнес өзгеру кестесі;

Нақты ақпараттандыру объектілері үшін шешім қабылдауды қолдау жүйесі модульдерін тестілеу орындалды (енгізу актілері қосымшада келтірілген). «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі тестілеу барысында ақпараттандыру объектілерінің ақпараттық-коммуникациялық жүйе үшін киберқауіпсіздік құралдарын орналастырудың ұтымды нұсқаларын таңдау бойынша есептеу эксперименттері орындалды. Бұл, атап айтқанда, шектеулі жағдайларда қорғаныс ресурстарын қайта бөлу есебін шешу үшін қажет; «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі қолдану аппараттық-бағдарламалық ақпаратты қорғау құралдары және олардың ақпараттық-коммуникациялық жүйеге арналған комбинацияларының әртүрлі нұсқаларын жылдам сұрыптауды орындауға ғана емес, сонымен бірге олардың ерекшелігіне қарай ақпараттандыру объектісі үшін ақпараттық-коммуникациялық жүйе киберқауіпсіздік контурларының құрамын оңтайландыру бойынша қолда бар модельдермен және алгоритмдермен келтірілген модельдер мен алгоритмдерді біріктіруге мүмкіндік беретіні көрсетілген. Модельдер мен алгоритмдердің мұндай бірігуі ақпараттық-коммуникациялық жүйе қорғанысын тез қалпына келтіруге мүмкіндік береді; Монографияның 4-тарауында өткізілген «Decision support systems Dynamic allocation of cyber security resources» шешім қабылдауды қолдау жүйесі мүмкіндіктерінің практикалық құндылығы ақпараттың жоғалуынан болатын тәуекелдердің жиынтық шамасын, ақпаратты қорғау құралдары интегралды көрсеткіштерін, ақпаратты қорғау құралдарының әрбір сыныбы үшін құндық көрсеткіштерін, сондай-ақ, ақпаратты жоғалтудан

туындайтын тәуекелдердің жиынтық шамасын ескере отырып, ұсынылған генетикалық алгоритм негізінде шешім қабылдауды қолдау жүйесі үшін есептеуіш өзек үшін оның архитектурасына серпінді қосылатын кітапханаларды қосу мүмкіндігімен шешім қабылдауды қолдау жүйесі ашық көп модульді архитектурасын бағдарламалық іске асырудың нәтижелілігін растады. Тарау шеңберінде жүргізілген есептеу эксперименттері шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда ақпараттандыру объектісін қорғау тарапының ресурстарын бөлуді оңтайландыруға мүмкіндік берді.

МОНОГРАФИЯ БОЙЫНША ҚОРЫТЫНДЫ

Бұл монографиялық зерттеуде ақпараттық-коммуникациялық жүйелердің (АКЖ) киберқауіпсіздігін қамтамасыз етуге арналған модельдер, әдістер және алгоритмдер кешенді түрде талданды. Зерттеу барысында келесі негізгі нәтижелер мен ғылыми тұжырымдар алынды.

ISO / IEC TR 13335 сәйкес ақпараттық-коммуникациялық технологиялар сегменті ретінде ақпараттық-коммуникациялық жүйе қауіпсіздігін басқару модельдері талданды. ISO/ IEC 27001: 2010 сәйкес «жоспарла - орында – тексер - әрекет ет» моделінің мазмұны ашылды. Ақпараттандыру объектісі ақпараттық қауіпсіздік және оның ақпараттық-коммуникациялық жүйе басқару құрылымы ақпараттың өмірлік циклі деңгейінде «объект - қауіп - қорғау» тұжырымдамасына және «кибернетикалық кеңістік – коммуникациялық орта - физикалық кеңістік» көп деңгейлі моделіне сәйкес талданды. Қолданыстағы ақпаратты қорғау құралдары оңтайландыру модельдерін талдау қарастырылған модельдердің көпшілігінің мақсаты ақпараттық қауіпсіздікке жалпы шығындарды оңтайландыру екенін көрсетті (Гордон-Леб моделі, К.Задираки моделі). Тек бір ғана модельдер серпінді режимде ақпараттық қауіпсіздік (Глушак-Новиков моделі) объектілері арасында оңтайлы қаражат бөлуді іздеуге бағытталған.

Ақпараттандыру объектісі объектілерінде ақпараттық ресурстардың қауіптері мен осалдығын іске асырудан келтірілген залалды сипаттайтын модельдің мақсатты функциясын таңдау негізделген. Бөлшек-сызықтық функциялар материалдық тасымалдаушыларда сақталатын ақпараттың осалдығын сипаттайды, мұнда ақпаратты қорғауға, сондай-ақ ұйымдастырушылық және инженерлік-техникалық іс-шаралар мен қорғаныс құралдарына бөлінетін ресурстардың ұлғаюы, қорғаныс жағы ресурстарының мәндерінің бастапқы саласында монотонды, осалдықтың пропорционалды төмендеуіне және нәтижесінде - ақпараттандыру объектісі үшін зиян мөлшерін азайтуға әкеледі. Бөлшек сызықты емес функциялар кедергілерді жеңу үшін айтарлықтай ресурстар қажет болатын компьютерлік жүйелерде таратылатын ақпараттың қасиеттерін көрсететіні анықталды.

Сонымен қатар жаңартылған генетикалық алгоритмді қолдану ұсынылды. Жаңғыртылған генетикалық алгоритмде қолданыстағыларға қарағанда, анық емес қатынастармен кибернетикалық қауіпсіздікті қамтамасыз ету жөніндегі жобаларды іске асыру процесінде қорғау тарапының ресурстарын бөлуді оңтайландырудың көп критерийліесепін шешу үшін Беллман-Заде қағидаты қолданылды. Бұл ақпараттандыру объектісі құрамындағы компоненттердің осалдықтарын төмендетуге бағытталған іс-шаралармен байланысты жұмыстарға ресурстарды бөлуді оңтайландыруға және шабуылдаушы тараптың ресурстары туралы деректер болмаған жағдайда ақпараттандыру объектісі қорғанысының берілген мәндеріне қол жеткізуді қамтамасыз ететін ресурстар көлемінің әртүрлі нұсқаларын модельдеуге мүмкіндік береді.

IIoT (Industrial Internet of Things) инфрақұрылымы бойынша алынған нәтижелер).IoT хаттамалары: MQTT over TCP өндірістік орта үшін ең тиімді екені, MQTT over WebSocket веб-қосымшаларда қолайлы екені, ал HTTP протоколы кідірістері себебінен тиімсіз екені көрсетілді. Цифрлық егіздер: өндірістік процестерді модельдеу кезінде цифрлық егіздер арқылы желідегі аномалияларды нақты уақыт режимінде бақылау мүмкіндігі дәлелденді. Машиналық оқыту алгоритмдері: Random Forest 99.82% дәлдікке жетіп, шабуылдарды жіктеуде ең сенімді әдіс екені анықталды. KNN және логистикалық регрессия да сыналды, бірақ олардың нәтижелері төменірек болды. Терең оқыту әдістері: LSTM және CNN-LSTM сенсорлық аномалияларды анықтауда жоғары нәтижелер көрсетті. CNN-LSTM шамамен 92% дәлдікке қол жеткізді. Бұл IIoT деректеріндегі уақыттық және кеңістіктік байланыстарды тиімді анықтай алатынын көрсетті. Edge AI интеграциясы: деректерді бұлтқа жібермей, тікелей құрылғы деңгейінде өңдеу арқылы (edge computing) қауіпсіздік деңгейін арттыруға және кідірістерді азайтуға болатыны дәлелденді.Қорғаныс шаралары: TLS/SSL шифрлау, RBAC негізіндегі қол жеткізуді басқару, IDS/IDPS жүйелерін біріктіру IIoT киберқауіпсіздігін кешенді қорғауды қамтамасыз ететіні негізделді.

Ақпараттық-коммуникациялық жүйелердің қауіпсіздік контурлары үшін ақпаратты қорғау құралдарының конфигурацияларының нұсқаларын іріктеумен және оңтайландырумен байланысты есептерді шешу үшін генетикалық алгоритмді дамытуды алды.

Осы нәтижелердің ғылыми жаңалығы – генетикалық алгоритмде ақпаратты қорғау құралдары құрамын оңтайландыру үшін критерийлар ретінде ақпаратты жоғалтудан болатын тәуекелдердің жиынтық шамасын, ақпаратты қорғау құралдары интегралды көрсеткіштерін, сондай-ақ әрбір ақпаратты қорғау құралдары класы үшін құндық көрсеткіштерді пайдалану ұсынылатындығында. Ақпараттық-коммуникациялық жүйеге арналған ақпаратты қорғау құралдары құрамын таңдауды оңтайландыру есебіндегі генетикалық алгоритм көп таңдаумен байланысты есептің вариациясы ретінде қарастырылады. Бұл өндірісте ақпаратты қорғау құралдарын ақпараттық-коммуникациялық жүйе - қорғаныс контурлары бойынша орналастыруды оңтайландыру рюкзактың комбинаторлық есепін өзгерту ретінде қарастырылады. Ұсынылған тәсіл ақпараттық-коммуникациялық жүйе түйіндерінің әрқайсысы үшін ақпаратты қорғау құралдары жиынтығын оңтайландыру жөніндегі көп критерийліесепті шешуге ғана емес, сонымен қатар ақпаратты қорғау құралдары киберқауіпсіздік бөлінетін ресурстардың шектеулілігі жағдайында қорғау тарабының ресурстарын қайта бөлудің орындылығына жедел талдау жүргізуге мүмкіндік береді. Зерттеудің осы бөлігінің практикалық құндылығы ақпаратты жоғалту, ақпаратты қорғау құралдары интегралдық көрсеткіштері, сондай-ақ ақпаратты қорғау құралдарының әрбір класы үшін құндық көрсеткіштері тәуекелдерінің ұсынылған модификациясы негізінде шешім қабылдауды қолдау жүйесі есептеу өзегі үшін серпінді қосылатын кітапхана түрінде модульді бағдарламалық іске асыруда болып табылады. Есептеу эксперименттері барысында модификацияланған генетикалық алгоритмді іске асыру ақпараттық-коммуникациялық жүйеге арналған киберқауіпсіздік құралдарын орналастырудың оңтайлы нұсқаларын іздестіруді жеделдетуге, сондай-ақ қорғау ресурстарын олардың шектеулілігі жағдайында қайта бөлу жөніндегі есепті шешуге мүмкіндік беретіні анықталды. Бұл артықшылық аппараттық және бағдарламалық жасақтаманың әртүрлі нұсқаларын және олардың ақпараттық-коммуникациялық жүйеге арналған комбинацияларын жылдам сұрыптап қана қоймай, сонымен бірге тарауда келтірілген модельдер мен алгоритмдерді ақпараттық-коммуникациялық жүйе киберқауіпсіздік контурларының құрамын оңтайландыру үшін қол жетімді модельдер мен алгоритмдермен біріктіруге

мүмкіндік береді. Модельдер мен алгоритмдердің мұндай бірігуі ақпараттық-коммуникациялық жүйе қорғанысын тез қалпына келтіруге мүмкіндік береді.

Ақпаратты қорғау тарапымен ресурстарды бөлудің ұтымды нұсқасын талдау және таңдау барысында шешім қабылдауды қолдау жүйесі құрылымдық схемасы ұсынылды. Шабуыл жасайтын тараппен серпінді қарсыласу жағдайына баса назар аударылады. Осыған ұқсас негізгі функционалдық модульдер қарастырылды. Шешім қабылдауды қолдау жүйесі модульдік архитектурасы жүйенің үздіксіз және тиімді жұмыс істеуін қамтамасыз етуге ықпал етеді. «Decision support systems Dynamic allocation of cybersecurity resources» шешім қабылдауды қолдау жүйесі барлық жүйеден тұрады. «Decision support systems Dynamical location of cybersecurity resources» шешім қабылдауды қолдау жүйесі әзірлеумен байланысты осы нәтижелердің практикалық құндылығы ақпаратты жоғалтудан туындайтын тәуекелдердің жиынтық шамасын, ақпаратты қорғау құралдары интегралдық көрсеткіштерін, сондай-ақ ақпаратты қорғау құралдарының әрбір сыныбы үшін құндық көрсеткіштерін ескере отырып, ұсынылған генетикалық алгоритм негізінде шешім қабылдауды қолдау жүйесіне есептеуіш негіз үшін оның архитектурасына серпінді қосылатын кітапханаларды қосу мүмкіндігі бар шешім қабылдауды қолдау жүйесі ашық көп модульді архитектурасын бағдарламалық іске асырудың нәтижелілігін растады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Post, G. V., &Kagan, A. (2007). Evaluatinginformationsecuritytradeoffs: Restricting access can interfere with user tasks. Computers & Security, 26(3), 229-237.

2. Coull, A., Yzerbyt, V. Y., Castano, E., Paladino, M. P., &Leemans, V. (2001). Protecting the ingroup: Motivated allocation of cognitive resources in the presence of threatening ingroup members. Group Processes & Intergroup Relations, 4(4), 327-339.

3. Cappanera, P., &Scaparra, M. P. (2011). Optimal allocation of protective resources in shortest-path networks. Transportation Science, 45(1), 64-80.

4. Отчет за 2020 г. с результатами глобального опроса директоров по информационной безопасности https://www.cisco.com/c/ru_ru/products/security/security-reports.html

5. Годовой отчет компаний Cisco по информационной безопасности https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf

6.Отчет «Понимание киберугроз 2020» https://www.cloudav.ru/upload/iblock/b58/PandaLabs%20-%20 Threat-Insights-2020.pdf

7. Зегжда, П. Д., Полтавцева, М. А., & Лаврова, Д. С. (2017). Систематизация киберфизическихсистеми оценка из безопасности. Проблемы информационной безопасности. Компьютерные системы, (2), 127-138.

8. Дудикевич, В.Б., Никитин, Г. В., Ребец, А. И., & Мельник, М. В. (2019). Беспроводные сенсорные сети Zigbee, Wi-Fi и Bluetooth в киберфизичних системах: концепция объект-угроза-защита на основе модели OSI. Системы обработки информации (2), с. 114-120.

9. Калашников, А. О., & Аникина, Е. В. (2018). Модель управления информационной безопасностью критической информационной инфраструктуры на основе выявления аномальных состояний (Часть 2). Информация и безопасность, 21(2), с. 155-164.

10. Королев, М. (2010). Информационная безопасность предприятия. Вестник Института экономики Российской академии наук, (4), с. 187-191.

11. Евсеев, С. П., Коц, Г. П., & Король, О. Г. (2015). Анализ законодательной базы к системе управления информационной безопасностью НСМЭП. Восточно-Европейский журнал передовых технологий, (5 (3)), 48-59.

12. Буренин, А. Н., Легков, К. Е., &Оркин, В. В. (2018). Управление инцидентами при обеспечении безопасности информационных подсистем автоматизированных систем управления сложными организационно-техническими объектами. Инфокоммуникационныетехнологии, 16(1), 122-131.

13. Mataracioglu, T., &Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. arXiv preprint arXiv:1108.2150.

14. Sheikhpour, R., &Modiri, N. (2012). An approach to map COBIT processes to ISO/IEC 27001 information security management controls. International Journal of Security and Its Applications, 6(2), 13-28.

15. Котенко, И. В., &Новикова, Е. С. (2013). Методики визуального анализа в системах управления информационной безопасностью компьютерных сетей. Вопросы защиты информации, (3), 33-42.

16. Баранова, Е. К. (2015). Методики анализа и оценки рисков информационной безопасности. Образовательные ресурсы и технологии, (1 (9)). С. 73-79.

17. Шахалов, И. Ю., & Дорофеев, А. В. (2013). Основы управления информационной безопасностью современной организации. Правовая информатика, (3). С. 6-16.

18. Штеренберг, С. И., Виткова, Л. А., &Просихин, В. П. (2014). Методика применения концепции адаптивной саморазвивающейся системы. Информационные технологии и телекоммуникации, (4), 126-133.

19. Дидрих, В. Е., Дидрих, И. В., Громов, Ю. Ю., & Ивановский, М. А. (2016). Задача распределения ресурсов в сетевой информационной системе. Вестник Тамбовского государственного технического университета, 22(4). С. 541-547.

20. Лившиц, И. И. (2013). Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI/ISO. Информатизация и связь, (6), 62-67.

21. Глухова, Л. В., & Губанова, С. Е. (2015). Некоторые аспекты менеджмента информационной безопасности промышленных комплексов. Вестник Волжского университета им. ВН Татищева, (3 (34)). С. 1-10.

22. Siponen, M., &Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.

23. Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in cybersecurity: insights from the Gordon-Loeb model. Journal of Information Security, 7(02), 49.

24. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005.

25. Kramer, A. D. (2010, April). An unobtrusive behavioral model of» gross national happiness». In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 287-290).

26. Бабич, М. Д., Задирака, В. К., Людвиченко, В. А., & Сергиенко, И. В. (2010). Об использовании резервов оптимизации вычислений в компьютерных технологиях решения задач прикладной и вычислительной математики с требуемыми значениями характеристик качества. Журнал вычислительной математики и математической физики, 50(12), 2285-2295.

27. Фомченкова, Л. В., & Леонов, А. В. (2019). Модель управления информационной безопасностью. Экономика и бизнес: теория и практика, (12-3). с. 106-109.

28. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

29. Котенко, И. В. (2009). Интеллектуальные механизмы управления кибербезопасностью. Труды Института системного анализа Российской академии наук, 41, 74-103.

30. Десницкий, В. А., & Котенко, И. В. (2008). Модель защиты программного обеспечения на основе механизма» удаленного доверия». Известия высших учебных заведений. Приборостроение, 51(11).

31. Глушак, В. В., &Новіков, О. М. (2013). Синтез структуры системы защиты информации с использованием позиционной игры защитника и злоумышленника. Системнідослідження та інформаційнітехнології, (2), 89-100.

32. Глушак, В. В., Новиков, А. М., & Новиков, А. Н. (2013). Синтез структуры системы защиты информации с использованием позиционной игры защитника и злоумышленника. Системные исследования и информационные технологии, 2013, № 2. с. 89-100.

34. Скиба, А. В., & Архипов, О. Е. (2016). Информационные риски: модели рисков, исследование и использование. Инвестиции: практика и рпыт, (1), 51-60.

35. Лахно, В. А., Петров, А. С., &Чертунина, Н. Т. (2006). Исследование конфликтных потоков заявок в системах защиты информации. IEEE Journal on Selected Areas in Communications (JSAC), 24(2), 370-380.

36. Akhmetov, B., Lakhno, V., Akhmetov, B., &Alimseitova, Z. (2018, September). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162-171). Springer, Cham.

37. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.

38. Ashenden, D. (2008). Information Security management: A human challenge?. Information security technical report, 13(4), 195-201.

39. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. information security technical report, 13(4), 247-255.

40. Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. IEEE Security& Privacy, 5(1), 36-44.

41. Кононович В., Тардаскина Т. Алгоритм распределения ресурсов информационной безопасности документальных телекоммуникаций. Прав., Нормативы. и метрол. обеспе. системы защиты информации в Украине. 2004. Вып. 9. С. 152-161.

42. Белов С. В., Попова Е. А., Кальнов М. В. Формализация задачи распределения ресурсов между различными функциями обеспечения защиты информации. Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2012. № 1. С. 112–116.

43. Быков А. Ю., Шматова Е. С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов. Наука и образование. 2015. Вып. № 9. С. 160–187.

44. Oh, S. J., Fritz, M., &Schiele, B. (2017, October). Adversarial image perturbation for privacy protection a game theory perspective. In 2017 IEEE International Conference on Computer Vision (ICCV) (pp. 1491-1500). IEEE.

45. Zhu, Q., &Rass, S. (2018, January). Game theory meets network security: A tutorial. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 2163-2165).

46. Маслова Н. А., Мовчан А. В. Использование интеллектуальных агентов при решении задач распределения ресурсов. Искусственный интеллект. 2014. № 3. С. 80-89.

47. Ojamaa, A., Tyugu, E., &Kivimaa, J. (2008, November). Pareto-optimal situaton analysis for selection of security measures. In MILCOM 2008-2008 IEEE Military Communications Conference (pp. 1-7). IEEE.

48. Turskis, Z., Zavadskas, E. K., &Peldschus, F. (2009). Multi-criteria optimization system for decision making in construction design and management. Engineering economics, 61(1). 7-17.

49. Rathgeb, C., Breitinger, F., & Busch, C. (2013, June). Alignment-free cancelable iris biometric templates based on adaptive bloom filters. In 2013 international conference on biometrics (ICB) (pp. 1-8). IEEE.

50. Kopel, D. B. (1993). Peril or Protection-The Risks and Benefits of Handgun Prohibition. Louis U. Pub. L. Rev., 12, 285.

51. Kotenko, I., Sineshchuk, Y., &Saenko, I. (2020, March). Optimizing Secure Information Interaction in Distributed Computing Systems by the Sequential Concessions Method. In 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP) (pp. 429-432). IEEE.

52. Grabaum, R., & Meyer, B. C. (1998). Multicriteria optimization of landscapes using GIS-based functional assessments. Landscape and urban planning, 43(1-3), 21-34.

53. Rajbhandari, S., Hodgins, S., Sanghvi, H., McPherson, R., Pradhan, Y. V., Baqui, A. H., & Misoprostol Study Group. (2010). Expanding uterotonic protection following childbirth through community-based distribution of misoprostol: operations research study in Nepal. International Journal of Gynecology & Obstetrics, 108(3), 282-288.

54. Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., &Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339.

55. Jana, D. K., & Ghosh, R. (2018). Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security. Journal of information security and applications, 40, 173-182.

56. Vinayakumar, R., Soman, K. P., &Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1222-1228). IEEE.

57. Overbye, T. J., Mao, Z., Shetye, K. S., & Weber, J. D. (2017, February). An interactive, extensible environment for power system simulation on the PMU time frame with a cyber security application. In 2017 IEEE Texas Power and Energy Conference (TPEC) (pp. 1-6). IEEE.

58. Kusyk, J., Uyar, M. U., &Sahin, C. S. (2018). Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks. Evolutionary Intelligence, 10(3-4), 95-117.

59. Адилжанова С. А., Тюлепбердинова Г.А., Газиз Г., Сакыпбекова М.Ж. Ақпараттандыру объетілерінің киберқауіпсіздік ресурстарының динамикалық басқарудың математикалық әдістерін талдау //Вестник КазНИТУ им.Сатпаева №3 (139). – 2020. –С. 102-106

60. He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., &Gabrys, B. (2016). The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence.

61. Abraham, A., Grosan, C., & Chen, Y. (2005). Cyber security and the evolution of intrusion detection systems. Journal of Engineering and Technology, ISSN, 0973-2632.

62. Зейнельгабдин, А. Б., &Исабаева, С. Б. (2019). Кибербезопасность Казахстана в период цифровой трансформации. Государственныйаудит, №4(45). С. 47-55.

63. Перевозчиков, А. Г., Решетов, В. Ю., & Лесик, А. И. (2017). Многошаговое обобщение модели» нападение-оборона». Вестник Тверского государственного университета. Серия: Прикладная математика, (2), 89-100.

64. Перевозчиков, А. Г., Решетов, В. Ю., & Лесик, А. И. (2018). Неоднородная игра «нападение-оборона» на основе обобщенного принципа уравнивания. Вестник Тверского государственного университета. Серия: Прикладная математика, (1), 89-106.

65. Грищук Р.В. Теоретические основы моделирования процессов нападения на информацию методами теории дифференциальных игр и дифференциальных преобразований: Монография / Р.В. Грищук. - Житомир: Рута, 2010. – 280 с.

66. Lakhno, V., Bereke, M., Adilzhanova, S., Desiatko, A., Palaguta, K. Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. Journal of Theoretical and Applied Information Technology, 2022, 100(7), p. 1693–1705

67. Грищук, Р. В. (2012). Использование дифференциальных игр для оптимизации управления в системах защиты информации / Грищук Р.В., Хорошко В.А., Хохлачева Ю.Е. Современная защита информации (2), с. 21–26.

66. Васин А.А. Теория игр и модели математической экономики. / А.А.Васин, В.В.Морозов. – М.: МАКС Пресс. – 2005. – 272 с.

68. Свиридов, В. И., & Моисеев, С. И. (2019). Математические модели оптимального распределения защитных ресурсов по источникам информационных угроз. Вестник Воронежского института высоких технологий, (1), 110-112.

69. Быков, А. Ю., & Шматова, Е. С. (2015). Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов. Машиностроение и компьютерные технологии, (9). С. 160-187.

70. Котенко, И. В., & Степашкин, М. В. (2004). Обманные системы для защиты информационных ресурсов в компьютерных сетях. Труды СПИИРАН, 1(2), 211-230.

71. Гладков, Л. А., Курейчик, В. В., & Курейчик, В. М. (2010). Генетические алгоритмы. Учебник. 2-е изд., испр. и доп. – М.: Физматлит, 2010. – 368 с.

72. Akhmetov, B., Lakhno, V., Chubaievskyi, V., Adilzhanova, S., Ydyryshbayeva, M.. Automation of Information Security Risk Assessment International Journal of Electronics and Telecommunications , 2022, 68(3), p. 549–555

73. Beketova, G. S., Akhmetov, B. S., Korchenko, A. G., & Lakhno, A. V. (2017). Optimization backup model for critical important information systems. Bulletin of the national academy of sciences of the republic of Kazakhstan, (5), 37–44.

74. Братченко, А. И., Бутусов, И. В., Кобелян, А. М., & Романов, А. А. (2019). Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления. Вопросы кибербезопасности, (1 (29)). с. 18–23.

75. Шматко, А. В., & Сычев, Е. В. (2011). Многокритериальный выбор систем защиты информации с помощью нечетких парных сравнений альтернатив. Системы обработки информации (3), с. 161–164.

76. Ногин, В. Д. (2004). Упрощенный вариант метода анализа иерархий на основе нелинейной свертки критериев. *Журнал вычислительной математики и математической физики*, *44*(7), с. 1261–1270.

77. Шляпкин, А. В. (2014). Метод оценки экономической эффективности подразделения по защите информации. Информационные системы и технологии: управление и безопасность, (3), с. 318–324.

78. Клевцов, С. И., Клевцова, А. Б., & Буринов, С. В. (2015). Модель параметрической качественной иерархической оценки состояния технической системы. Инженерный вестник Дона, 37(3). с. 1–18.

79. Chiba, Z., Abghour, N., Moussaid, K., El Omri, A., &Rida, M. (2019). New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security, 11(1), 61–84.

80. Nozaki, Y., & Yoshikawa, M. (2019). Security evaluation of ring oscillator puf against genetic algorithm based modeling attack. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 338–347). Springer, Cham.

81. S. Adilzhanova, A. Rakhysh, G. Amirkanova, G. Tyulepberdinova, M. Kunelbayev, and B. Ilessova, “Improving Critical Infrastructure Protection: Assessment Methods, AI, Digital Twins,” in *Proc. 7th Asia Conf. Cogn. Eng. Intell. Interact. (CEII)*, 2024, pp. 130–134. https://doi.org/10.1109/CEII65291.2024.00033

82. Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Transactions on Industrial Informatics, 15(7), 4362–4369.

83. Sureshkumar, T., Anand, B., &Premkumar, T. (2019). Efficient Non-Dominated Multi-Objective Genetic Algorithm (NDMGA) and network security policy enforcement for Policy Space Analysis (PSA). Computer Communications, 138, 90–97.

84. Llansó, T., McNeil, M., &Noteboom, C. (2019). Multi-Criteria Selection of Capability-Based Cybersecurity Solutions. In Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 7322–7330.

85. Ахметов Б.С., Адилжанова С.А., Абуова А.К., Сагындыкова Ш.. Қорғаныс объектілері арасында ресурстарды бөлуді оңтайландыру кезінде шешім қабылдауды қолдаудың модульдік жүйесі. Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы, №4(76), 2020 с. 128-135

86. Yan, D., Liu, F., Zhang, Y., Jia, K., & Zhang, Y. (2018). Characterizing the Optimal Attack Strategy Decision in Cyber Epidemic Attacks with Limited Resources. In International Conference on Science of Cyber Security (pp. 65–80). Springer, Cham.

87. Lee, Y., Choi, T. J., &Ahn, C. W. (2019). Multi-objective evolutionary approach to select security solutions. CAAI Transactions on Intelligence Technology, 2(2), 64-67.

88. Akhmetov, B., Lakhno, V., Akhmetov, B., &Alimseitova, Z. (2018). Development of sectoral intellectualized expert systems and decision making support

systems in cybersecurity. In Proceedings of the Computational Methods in Systems and Software (pp. 162–171). Springer, Cham.

89. Обзоры средств защиты информации (СЗИ). Источник:https://www.anti-malware.ru/reviews

90. Lakhno, V., Akhmetov, B., Malyukov, V., &Kartbayev, T. S. (2018). Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium of a bilinear multistep quality game with several terminal surfaces. International Journal of Electronics and Telecommunications, *64*(4), 467-472.

91. Биллиг, В. А. (2006). Основыпрограммирования на C#. М.: Изд-во «Интернет-университетинформационныхтехнологий-ИНТУИТ. 870 с

92. Tapiwa Gundu (2024) Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model

93. D. Saxena, A.K. Singh (2020). Security embedded dynamic resource allocation model for cloud data centre. ELECTRONICS LETTERS No. 20 pp. 1062–1065

94. Лахно В.А., Адилжанова С.А.. Генетикалық алгоритмді кибер қауіпсіздік ресурстарының динамикалық бақылау есептерінде қолдану Вестник КазНИТУ им.Сатпаева №6 (142). 2020. С. 565-568

95.Ахметов Б.С., Адилжанова С.А., Абуова А.К., Сагындыкова Ш. Қорғаныс объектілері арасында ресурстарды бөлуді оңтайландыру кезінде шешім қабылдауды қолдаудың модульдік жүйесі. // Абай атындағы ҚазҰПУ-нің хабаршысы, «Физика-математика ғылымдары» сериясы, №4(76), 2020 с. 128-135

96.Naveen Kumar Thawait. (2024) Machine Learning in Cybersecurity : Applications, Challenges and Future Directions. International Journal of Scientific Research in Computer Science Engineering and Information Technology 10(3):16-27

97.Ахметов Б.С.,. Адилжанова С.А, Лахно В.А., Сауанова К.Т. Ақпаратты қорғау тарапының ресурстарын іріктеу, оңтайландыру және қайта бөлу мәселесін шешу үшін генетикалық алгоритмді дамыту// Вестник АУЭС, Серия «Информационные, телекоммуникационные и космические технологии». – 2022. – №1 (56). – С.116-123.

98. Nadir Ali, William Jack. (2022). Reinforcement Learning for Adaptive Cybersecurity: A SelfLearning Approach to Threat Mitigation. DOI: 10.13140/ RG.2.2.28644.2880

99. Bauyrzhan Amirkhanov, Gulshat Amirkhanova, Murat Kunelbayev, Saltanat Adilzhanova, Miras Tokhtassyn. Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration// International Journal of Innovative Research and Scientific Studies (IJIRSS) Vol. 8 No. 1 (2025). pages: 679-694, https://doi.org/10.53894/ ijirss.v8i1.4414

100. Saltanat Adilzhanova , Murat Kunelbayev , Gulshat Amirkhanova , Yesset Zhussupov, Alikhan Tortay. Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise//International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 176-196 https://doi.org/10.53894/ijirss.v8i2.5136

101. S. Adilzhanova, M. Kunelbayev, G. Amirkanova, G. Tyulepberdinova, and D. Sybanova, “Analysis of the dynamics of cyberattacks and fraud methods using machine learning algorithms for IIoT: Information security of digital twins in Industry 4.0,” Int. J. Innov. Res. Sci. Stud., vol. 8, no. 2, pp. 4012–4026, 2025. https://doi.org/10.53894/ijirss.v8i2.6201

Ғылыми басылым

Адилжанова Салтанат Альмуханбетовна

КИБЕРҚАУІПСІЗДІК РЕСУРСТАРЫН АДАПТИВТІ БАСҚАРУҒА АРНАЛҒАН ЗАМАНАУИ ТӘСІЛДЕР МЕН ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАР

Монография

ИБ №16018
Басуға 13.10.2025 жылы қол қойылды. Пішімі 60x84 $^{1}/_{16}$.
Көлемі 10,12 б.т. Офсетті қағаз. Сандық басылыс. Тапсырыс №1909.
Таралымы 500 дана. Бағасы келісімді.
Әл-Фараби атындағы Қазақ ұлттық университетінің
«Қазақ университеті» баспа үйі.
050040, Алматы қаласы, әл-Фараби даңғылы, 71.

«Қазақ университеті» баспа үйі баспаханасында басылды.

ISBN 978-601-04-7297-6