ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ Ұлттық Техникалық зерттеу Университеті

Кибернетика және ақпараттық технологиялар институты

“Киберқауіпсіздік, ақпаратты өңдеу және сақтау” кафедрасы

Есен Жалғас Айдынұлы

Ақпараттандыру объектісін кешенді техникалық қорғау жүйесін әзірлеу

ДИПЛОМДЫҚ ЖҰМЫС

Мамандық 5В100200 – Ақпарттық қауіпсіздік жүйелері

Алматы 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И. Сәтбаев атындағы Қазақ Ұлттық Техникалық зерттеу Университеті
Кибернетика және ақпараттық технологиялар институты
“Киберқауіпсіздік, ақпаратты өңдеу және сақтау” кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі
техн.ғыл.канд. ассист.проф.
_____ Н.А.Сейлова
«03» 06 2021ж.

Дипломдық жобаға

ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: Ақпараттандыру объектісін кешенді техникалық қорғау жүйесін әзірлеу

5В100200-«Ақпараттық қауіпсіздік жүйелері»

Орындаған Есен Жалғас

Ғылыми жетекші магистр,сениор-лектор
Батырғалиев А.Б.
«02» 06 2021ж

Алматы 2021

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Ақпараттық қауіпсіздік кафедрасы

5В100200-«Ақпараттық қауіпсіздік жүйелері»

БЕКІТЕМІН
Кафедра меңгерушісі
техн.ғыл.канд.,ассист.проф.
_____Н.А. Сейлова
«03» 06 2021ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы: Есен Жалғас Айдынұлы
Тақырыбы: Ақпараттандыру объектісін кешенді техникалық қорғау жүйесін әзірлеу
Университет ректорының *"24"11 №2131-б бұйрығымен бекітілген*
Аяқталған жұмысты тапсыру мерзімі *2020жылғы "15"мамыр*
Дипломдық жобаның бастап берілістері
Дипломдық жобада қарастырылатын мәселелер тізімі
Ақпараттық қауіпсіздік және ақпараттық қауіпсіздік туралы негізгі түсініктер
Құпия ақпаратты өңдеудің заманауи автоматтандырылған жүйелері

Дипломдық жобаны орындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімдері	Ескерту
Құпия ақпаратты қорғау сертификатциясы	01.03.2021 г.	
Ақпаратты қорғау әдістері мен құралдары	26.03.2021 г.	
Кешенді техникалық қорғау жүйесін жасау	26.04.2021 г.	

Аяқталған дипломдық жобаның және оларға қатысты диплом жобасының бөлімдерінің кеңесшілерінің және қалып бақылаушының қолтаңбалары

Бөлімдер атауы	Кеңес берушілер (аты-жөні, тегі, ғылыми дәрежесі, атағы)	Қолтаңба қойылған мерзімі	Қолы
Қалып бақылаушы	техн.ғыл. магистрі, ассистент Кабдуллин М.А.	19.05.2021	

Ғылыми жетекші _____ Батырғалиев А.Б.

Тапсырманы орындауға қабылдап алған студент Есен Ж.А.

Күні “24” 11 2020ж.

АҢДАТПА

Бұл жұмыста кәсіпорнында ақпараттық қауіпсіздік жүйесін дамытуға қатысты мәселелер қарастырылған. Жұмыс барысында ақпаратты қорғаудың қол жетімді құралдарына талдау жүргізілді, нәтижесінде ақпарат көздері мен тасымалдаушылар құрамы анықталды, ақпарат санаттарға бөлінді және ақпараттың тарау арналары анықталды . Ақпараттық қауіпсіздік аудиті шеңберінде кәсіпорынның ақпараттық қауіпсіздік мәселелері бойынша ағымдағы қызметі талданды , қорғау жүйесіндегі кемшіліктер анықталды және оларды жою жолдары көрсетілді.

АННОТАЦИЯ

В данном дипломном проекте рассматриваются вопросы, связанные с развитием систем защиты информации на предприятии. В ходе работы были проанализированы имеющиеся средства защиты информации, в результате были определены источники информации и каналы передачи, информация была разделена на категории и определены возможные каналы утечки информации. В рамках аудита информационной безопасности проанализирована текущая деятельность предприятия по вопросам информационной безопасности, дана оценка информационной системы организации , выявлены недостатки в системе защиты и пути их устранения в работе.

ANNOTATION

This thesis project addresses issues related to the development of information security systems at the enterprise. In the course of the work, the available means of protecting information were analyzed, as a result, sources of information and transmission channels were identified, information was divided into categories and possible channels of information leakage were identified. As part of the information security audit, the current activities of the enterprise on information security issues were analyzed, the information system of the organization that distributes deficiencies in the protection system are identified, ways of their elimination in the work are outlined.

МАЗМҰНЫ

Кіріспе		9
1	Ақпараттық қауіпсіздік және ақпараттық қауіпсіздік туралы негізгі түсініктер	10
1.1	Құпия ақпаратты өңдеудің заманауи автоматтандырылған жүйелері	16
2	Құпия ақпаратты қорғау құралдарын сертификаттау	17
3	Ақпаратты қорғау әдістері мен құралдары	18
4	Несиелік бюродағы ақпаратты кешенді техникалық қорғауды дамыту	21
4.1	Ұйымдық құрылым	21
4.2	Ақпараттық-коммуникациялық технологияларды қолдануға қойылатын талаптар	21
4.3	Ақпараттық қауіп моделін талдау	22
4.4	Несиелік бюро үшін техникалық қорғаудың кешенді жүйесін енгізу	24
4.5	Байланыс каналдары арқылы ақпараттың тарап кетуден қорғаудың техникалық құралдарын енгізу	25
Қорытынды		32
Пайдаланылған әдебиеттер тізімі		33

Кіріспе

Қазіргі таңда адамның жұмысын, кәсіпорынды ұйымдастыруды автоматтандырылған жүйелер мен процестерді еңгізбей елестету қиын. Сонымен қатар, әр маман өз жүйесін қарапайым және қолдануға ыңғайлы етуге тырысады, өйткені бұл нарықта бәсекелестік көп. Ақпараттық технологиялар саласы жыл сайын қарқынды дамып келеді. Жыл сайын өндірістік процестер автоматтандырылуда. Ғаламтор пайдаланушылар саны да үнемі өсіп келеді. Әрине, қазіргі кезде сирек кездесетін, тіпті ең қарапайым жүйе ғаламтор ресурстарын пайдаланбай жұмыс істемейді.

Ұйымның қауіпсіздігіне сыртқы әсерден басқа, ақпараттық байланыс арналары арқылы ақпараттың таралу қаупі бар. Тек сыртқы қауіпсіздік жеткіліксіз. Әр ұйым қызметіне қатысты ақпараттың тұтастығын, қол жетімділігі мен құпиялылығын қамтамасыз етуге тырысады. Осындай мәселелерді шешу үшін ақпараттық ресурстардың қауіпсіздігін қамтамасыз етудің кешенді тәсілін әзірлеу бағыты пайда болды. Ақпаратты кешенді қорғау қауіп-қатердің санын қысқартуға әсер етеді.

Ақпараттандыру объектісін кешенді қорғау жүйесі дегеніміз - бұл белгілі бір аумақта белгілі бір тәртіпті қамтамасыз етуге бағытталған техникалық құралдардың, оларды қолдану әдістерінің кешені.

Қазіргі таңда ақпаратты қорғау барған сайын күрделі мәселеге айналуда. Бұған қоса, қазіргі кезде ақпаратқа рұқсатсыз қол жеткізу құралдары мен әдістері кең таралған. Ақпараттың тарап кетуінің табиғи арналары өздігінен пайда болатынын есте ұстауымыз керек. Сондай-ақ, ақпарат алудың белсенді әдістерін қолдану арқылы ақпараттың жасанды тарау арналары пайда болады. Белсенді әдістер арнайы техникалық құралдарды қолдану арқылы ақпараттың жаңа техникалық тарау арналарын жасайды. Бұл - сымдарға және байланыс желілеріне заңсыз қосылу, техникалық қондырғылар орнату және техникалық құрылғыларда өңделетін немесе сақталатын ақпаратқа рұқсатсыз қол жеткізу болуы мүмкін.

Сондықтан ақпараттандыру объектісінің кешенді техникалық қорғау жүйесін құру шаралары әр кәсіпорынға қажет.

1 Ақпараттық қауіпсіздік және ақпараттық қауіпсіздік туралы негізгі түсініктер

Ақпаратты өңдеу, тарату және сақтаудың заманауи әдістері ақпаратты жоғалту, бұрмалау және жария ету қауіптерінің пайда болуына ықпал етеді. Сондықтан компьютерлік жүйелер мен желілердегі ақпараттарды қорғауды қамтамасыз ету, ақпараттық қауіпсіздікті дамытудағы жетекші бағыттардың бірі болып табылады. ҚР СТ 34.025-2006 анықтамаларын ескере отырып, компьютерлік жүйелер мен желілердің ақпараттық қауіпсіздігі мен ақпараттық қауіпсіздігінің негізгі анықтамаларына шолу.

Ақпаратты қорғау - тарап кетуді, ұрлауды, жоғалтуды, рұқсатсыз жоюды, өзгертуді, рұқсатсыз көшіруді болдырмау мақсатында қабылданған ұйымдастырушылық, құқықтық, технологиялық шаралар [1].

Автоматтандырылған жүйе - өзара байланысты компоненттердің жиынтығын құрайтын ұйымдық-техникалық жүйе. Мысалы: ақпаратты өңдеу мен сақтаудың техникалық құралдары, бағдарламалық қамтамасыз ету , өңдеу әдістері мен алгоритмдері, әр түрлі ақпарат құралдары [2].

Қауіпсіз автоматтандырылған жүйе - ақпаратты қорғау бойынша стандарттардың және нормативтік құжаттардың талаптарына сәйкес ақпараттық технологияларды іске асыратын автоматтандырылған жүйе [1].

Қауіп тобындағы ұйымдар

Қорғалған мәліметтердің жоғарыда аталған критерийлеріне сәйкес, ақпараттың таралуының негізгі қауіпі бар кәсіпорындардың бірнеше түрі бар. Ол:

- мемлекеттік құпияны құрайтын мәліметтермен жұмыс жасайтын коммерциялық және коммерциялық емес, ғылыми және басқа ұйымдар
- қаржылық қызметтер нарығында жұмыс істейтін, өз тұтынушыларының есепшоттары мен қаржылары, олардың банк карточкалары туралы мәліметтерге ие ұйымдар;
- ашық нарыққа шығатын, көптеген жеке деректермен жұмыс істейтін ұйымдар;
- өз жұмысында жаңа технологиялар қолданатын ұйымдар;

Олардың барлығы ақпараттың тарап кетуіне жол бермеудің қол жетімді әдістерін барынша тиімді пайдалануы керек, өйткені бұл жағдайда зиян тек заңды тұлғаға ғана емес, сонымен қатар тұтынушыларға да тиуі мүмкін. Кейбір жағдайларда кәсіпорын қорғаныс шараларын қолданбағаны үшін жауапкершілікке тартылуы мүмкін. Ақпараттың тарап кетуінің әр арнасы оның қауіпсіздігін анықтау тұрғысынан талданып, барынша қорғалуы керек.

Қауіпті толығымен жою үшін ықтимал шабуылдардың нысаны болып табылатын және қорғаныс құралдарының барлық спектрін ұсына алатын ең құнды деректер жиынтығын анықтай алатын мамандармен байланыс қажет.

Көрнекі-оптикалық құралдар

Монитордың экранын немесе үстелдің үстінде жатқан құжаттардың бір бөлігін кеңсе терезесінен көруге болатын болса, ақпараттың таралуының қаупі бар. Ақпарат көзінен шыққан кез-келген жарық ағыны ақпараттың заңсыз таралуына ықпал етеді. Бұл әдіспен күресу үшін көп жағдайда арнайы техникалық құралдарды қолдану қажет.

Акустикалық арналар

Дыбыс түріндегі ақпарат тарап кетуге өте осал. Ультра жиіліктегі дыбыс оңай таралады. Егер оның жолында кедергі болса, дыбыстық толқын ондағы тербелістерді тудырады және оларды арнайы құрылғылар оқиды. Дыбыстың бұл қасиеті ғимараттың немесе кеңсенің жобалау кезеңінде ескерілуі керек. Қауіпсіздік дәрежесін бағалау үшін стетоскоптар қолданылады.

Егер дыбыстың максималды жұтылуына қол жеткізу мүмкін болмаса, ғимараттың негізгі қабырғаларының периметрі бойынша, тыңдаудан қорғалмаған немесе жиналыс бөлмелерінде орнатуға болатын генераторларды қолдануға қажет.

Акустикалық ақпараттың тарап кетуі келіссөздер кезінде диктафон қолдану арқылы да іске асуы мүмкін. Олардың бар екенін анықтау үшін арнайы құрылғылар қолданылады. Телефондарда дауыстық сигналды алуға арналған қондырғыларды орнату қазір іс жүзінде қолданылмайды, цифрлық трафикті ұстау басқа жолмен, соның ішінде телефон операторы немесе интернет-провайдер арқылы қолданылады. Бұл қауіп дәрежесін, телефон сұхбатында талқылауға болатын құпия ақпарат туралы арнайы нұсқаулар жасау арқылы да ескеру қажет.

Электромагниттік арналар және байланыс арналары

Жалған электромагниттік сәулеленудің ақпаратының тарап кетуі де қауіпті. Электромагниттік өрісте қысқа қашықтықта таралатын электромагниттік толқындарды да ұстап алуға болады. Мысалға:

- телефондар мен домофондардың микрофондарынан;
- жерлендіру мен қоректендірудің негізгі желісінен;
- аналогтық телефон желісінен;
- талшықты-оптикалық байланыс арналарынан;
- басқа көздерден.

Оларды қорғау және дешифрлеу қазіргі заманғы техникалық құралдар үшін қиын емес.

Бұл жағдайда күресу әдістері сымдарды жерге қосу, электромагниттік сәулеленудің ең айқын көздерін қорғау, шабуыл құралдарын анықтау немесе шабуыл құралдарын анықтау үшін арнайы бағдарламалық және аппараттық құралдарды қолдануға болады. Мұнда ұрлықпен күресті техникалық құралдармен де, бағдарламалық құралдармен де жүргізуге болады.

Материалдық арналар

Қарапайым қоқыс немесе өндірістік қалдықтар деректердің құнды көзі бола алады. Бақыланатын аймақтан шығатын қалдықтар өндіріс технологиясы туралы маңызды ақпарат көзіне айналуы мүмкін. Осы қауіпке қарсы жүйені дамыту үшін қалдықтарды өңдеу технологияларын қолданумен бірге кешенді шешім қажет.

Ақпараттың тарап кетуінің жоғарыда аталған барлық әдістері ұры үшін дереккөздің аумақтық қол жетімділігін талап етеді, аудио немесе визуалды ақпаратты ұстауға арналған әдеттегі құрылғының жұмыс аймағы бірнеше ондаған метрден аспайды. Электромагниттік сәулеленуді және акустикалық тербелістерді жинауға арналған қондырғыларды орнату объектіге тікелей енуді қажет етеді. Оның орналасуын білу де қажет, бұл қызметкерді жалдауды талап етуі мүмкін. Кеңселердің көпшілігі бейнебақылау камераларымен жабдықталғанына қарамастан, қазіргі кезде бұл әдістер кеңінен қолданылады.

Ғаламтордың мүмкіндіктерін пайдаланатын ұрлықтың заманауи әдістерімен және оның көмегімен деректер мұрағаттарына немесе дауыстық трафикке қол жеткізу аса қауіпті болып табылады.

Ақпараттың тарап кетуіне жол бермеу тәсілдері

Ақпараттың таралуының жоғарыда аталған барлық әдістерінен тиімді қорғану үшін іс-шаралар мен шаралардың екі негізгі тобын қамтитын қауіпсіздік шаралар жүйесін әзірлеу қажет:

- әкімшілік-ұйымдастырушылық шаралар;
- техникалық және бағдарламалық шаралар.

Іс-шаралардың бірінші тобы да, екінші тобы да іске асырылғанға дейін кәсіпқойлардан міндетті түрде кеңес алу қажет, әсіресе егер компания мемлекеттік құпиямен жұмыс істеуге лицензия алғысы келсе. Қолданылатын техникалық құралдар Қазақстан Республикасы аумағында сертификатталған және мақұлданған болуы керек, ақпараттарды қорғау мақсатында «шпиондық бағдарламалар» санатына жататын, тексерілмеген немесе тыйым салынған құралдарды пайдалануға жол берілмейді. Ақпаратты қорғау тек заңды күрес әдістеріне негізделуі керек.

Қауіпсіздік жүйесі ұйымдастырушылық шараларға сүйене отырып, кешенді түрде жасалуы керек. Оның барлық элементтері бірыңғай кешенді

құрауы керек, оның орындалуын бақылау құзыретті қызметкерлерге жүктелуі керек.

Қорғау жүйесін жобалау принциптері

Құпия ақпаратты қорғаудың кешенді жүйесі негізделетін белгілі бір қағидалары бар:

- кеңістіктегі және уақыттағы жүйенің үздіксіздігі, қолданылатын қорғау әдістері белгілі бір қауіптердің пайда болуына немесе бақылау деңгейінің төмендеуіне жол бермеу, бүкіл материалды және ақпараттық периметрді тәулік бойы бақылау керек;

- ақпаратты маңыздылық дәрежесіне қарай бөліп, оны қорғау үшін әр түрлі әсер ету әдістерін қолдану керек;

- ақпараттың барлығы бірдей маңызды бола бермейді, сондықтан ең маңызды қауіпсіздік шаралары ең жоғары мәнге ие ақпаратқа қолданылуы керек;

- жүйенің барлық компоненттері бір-бірімен өзара әрекеттесіп, бір орталықтан басқарылуы керек. Егер компания холдингтік компания болса немесе оның бірнеше филиалы болса, бас компаниядан ақпараттық жүйелерді басқаруды құру қажет;

- барлық ең маңызды блоктар мен байланыс жүйелері қайталануы керек, сонда қорғаныс буындарының бірі бұзылған жағдайда оны басқару блогы ауысады.

Әкімшілік-ұйымдастырушылық шаралар

Қауіпсіздікті сақтау үшін кәсіпорын басшысы, сондай-ақ оның қауіпсіздік қызметіне жауапты орынбасарларының бірі үлкен жұмыс атқаруы қажет. Ақпараттық қауіпсіздіктің жалпы деңгейінің 70% -ы әкімшілік және техникалық шараларға байланысты, өйткені коммерциялық тыңшылық қызметінде қызметкерлерге пара беру жағдайларын пайдалану, ақпаратты ұрлауға арналған арнайы техникалық құралдарды қолданудан гөрі әлдеқайда кең таралған.

Құжаттарды әзірлеу

Коммерциялық құпияны және басқа ақпаратты қорғауға арналған ұйымның барлық ережелері ең қатаң талаптарға сәйкес келуі керек. Бұл осы типтегі құжаттаманы сапалы дайындау болашақта компанияның позициясы туралы даулар туындаған жағдайда сотта қорғауға мүмкіндік беретіндігімен байланысты.

Жеке құраммен жұмыс

Персонал кез-келген ақпараттың тарап кетуінен қорғаудың ең әлсіз буыны болып табылады. Бұл онымен жұмыс істеуге барынша назар аудару қажеттілігіне әкеледі. Мемлекеттік құпиямен жұмыс жасайтын компаниялар үшін арнайы рұқсат беру жүйесі бар. Басқа ұйымдар құпия деректермен жұмыс істеу мүмкіндігін шектеу үшін әр түрлі шаралар қабылдауы керек.

Коммерциялық құпияны құрайтын мәліметтер тізімін жасап, оны еңбек келісімшартына қосымша етіп енгізу қажет. Мәліметтер базасында қамтылған ақпаратпен жұмыс істеу кезінде қатынау жүйелері жасалуы керек.

Көшірудің барлық мүмкіндіктерін және сыртқы электрондық поштаға жіберуді шектеу қажет. Барлық қызметкерлер коммерциялық құпияны қамтитын ақпараттармен жұмыс істеу нұсқаулығымен таныс болуы және оны журналға жазу арқылы растауы керек. Бұл қажет болған жағдайда оларды жауапкершілікке тартуға мүмкіндік береді.

Нысанда қол жетімділік режимі барлық келушілердің мәліметтерін бекітуді ғана емес, сонымен қатар қауіпсіздік талаптарына жауап беретін күзет компанияларымен жұмысты қамтуы керек.

Контрагенттермен жұмыс

Ақпараттың таралуына көбіне қызметкерлер ғана емес, компанияның контрагенттері де қатысады. Бұл ақпараттық жүйелерді әзірлеу және қолдау бойынша қызмет көрсететін көптеген консалтингтік-аудиторлық компаниялар, фирмалар. Бұл қауіп өте маңызды деп бағалануы керек. Серверлік немесе бұлтты бағдарламалар арасында таңдау кезінде біріншісін таңдау керек. Майкрософттың мәліметінше, бұлт ресурстарына кибер шабуылдардың саны биыл 300%-ға артты.

Коммерциялық құпияны құрайтын мәліметтерді беруді талап ететін барлық контрагенттерге деген қажеттілік үлкен. Барлық келісімшарттарда оны ашқаны үшін жауапкершілікті көздейтін жағдайлар қарастырылуы керек.

Жоспарлау және техникалық шешімдер

Келіссөздер жүргізілетін немесе қорғалатын ақпарат орналасқан кеңсенің архитектурасын жоспарлау кезінде қорғау әдістеріне қойылатын барлық талаптарды сақтау қажет. Жиналыс бөлмелері қажетті сертификаттаудан өтуі керек, барлық заманауи экрандау әдістері, дыбыс сіңіретін материалдар, шу генераторлары қолданылуы керек.

Тарап кетудің алдын алу технологиясы мен жүйелері

Ақпаратты тарап кетуден немесе ұрлаудан қорғау үшін көптеген техникалық шараларды қолдану қажет. Қазіргі техникалық құралдар төрт топқа бөлінеді:

- инженерлік;
- техникалық құралдар;
- бағдарламалық жасақтама;
- криптографиялық құралдар.

Инженерлік

Қорғаныс құралдарының бұл санаты жоспарлау және сәулеттік шешімдерді жүзеге асыруда қолданылады. Олар бөтен адамдардың қорғалатын объектілерге, бейнебақылау жүйелеріне, дабыл сигнализацияларына, электронды құлыптарға және басқа да осыған ұқсас құрылғыларға кіру мүмкіндігін физикалық блоктайтын құрылғылар.

Техникалық құралдар

Оларға өлшеу құралдары, анализаторлар, ендірілген құрылғылардың орналасуын анықтауға мүмкіндік беретін техникалық құрылғылар, ақпараттың тарайтын арналарын анықтауға, олардың жұмысының тиімділігін бағалауға, мүмкін болатын жағдайдағы маңызды сипаттамаларды анықтайтын құралдар жатады. Олардың ішінде далалық индикаторлар, радиожиілікті өлшеуіштер, сызықтық емес локаторлар, аналогтық телефон желілерін сынауға арналған жабдықтар бар. Дауыс жазғыштарды анықтау үшін электромагниттік сәулеленуді анықтайтын детекторлар қолданылады, ал бейнекамера детекторлары сол принцип бойынша жұмыс істейді.

Бағдарламалық жасақтама

Бұл ең маңызды топтардың бірі, өйткені ол рұқсат етілмеген тұлғалардың ақпараттық желілерге кіруіне жол бермейді, хакерлік шабуылдарды бұғаттайды және ақпараттың таралуының алдын алады. Олардың ішінде жүйелік ақпараттық қорғауды қамтамасыз ететін арнайы бағдарламаларды атап өту қажет. Бұл DLP жүйелері және SIEM жүйелері, олар көбінесе ақпаратты қорғаудың кешенді механизмдерін жасау үшін қолданылады. DLP (Data Leak Prevention) құпия ақпараттың жоғалуынан толық қорғауды қамтамасыз етеді. Бүгінгі таңда олар негізінен периметрі бойынша, яғни хакерлерден емес, корпоративті желінің пайдаланушыларынан туындайтын қауіп-қатерлермен жұмыс істеуге арналған. Жүйелер ақпаратты жоғалту немесе түрлендіру нүктелерін анықтауға арналған кең ауқымды әдістерді қолданады және кез-келген рұқсат етілмеген кіруді немесе жіберуді блоктауға, оларды жіберудің барлық арналарын автоматты түрде тексеруге қабілетті. Олар пайдаланушының пошта трафигін, локальді қалталардың мазмұнын, мессенджерлердегі хабарламаларды талдайды және егер деректерді беру әрекеті анықталса, оны бұғаттайды.

SIEM жүйелері (Security Information and Event Management) желідегі ақпарат ағындары мен оқиғаларды басқарады, ал оқиға желіге және оның қауіпсіздігіне әсер етуі мүмкін кез-келген жағдай деп түсініледі. Ол пайда болған кезде, жүйе қауіп-қатерді жоюдың шешімін дербес ұсынады.

Бағдарламалық қамтамасыздандыру жеке мәселелерді шеше алады және компьютерлік желілердің күрделі қауіпсіздігін қамтамасыз ете алады.

Криптографиялық

Бұл санат желілер арқылы берілетін немесе серверде сақталатын барлық ақпаратты шифрлау алгоритмдерін ұсынады.

Қорғаныс әдістерінің барлық кешенін қолдану кейде артық болуы мүмкін, сондықтан белгілі бір компанияда ақпаратты қорғау жүйелерін ұйымдастыру үшін әр кәсіпорын жеке жобасын жасау керек, ол ресурстар тұрғысынан оңтайлы болып шығады.

1.1 Құпия ақпаратты өңдеудің заманауи автоматтандырылған жүйелері

Құпия ақпаратты өңдеудің заманауи автоматтандырылған жүйесі дегеніміз - бұл өзара байланысқан және мәліметтермен алмасатын, әр түрлі дәрежедегі көптеген компоненттерден тұратын күрделі жүйе. Кез-келген компонент зақымдалуы немесе бұзылуы мүмкін. Автоматтандырылған жүйенің компоненттерін келесі топтарға бөлуге болады [3]:

Аппараттық құралдар - компьютерлер және олардың компоненттері (процессорлар, мониторлар, терминалдар, перифериялық құрылғылар - диск жетектері, принтерлер, контроллерлер, кабельдер, байланыс желілері және т.б.).

Бағдарламалық жасақтама - әртүрлі бағдарламалар, утилиталар және т.б.

Персонал - жүйені пайдаланушылар және қызмет көрсетушілер.

Автоматтандырылған жүйенің барлық компоненттерінің қауіпсіздігін қамтамасыз ету үшін құпия ақпаратты қорғау жүйесін дамытуға кешенді тәсіл қажет. Сондай-ақ, жүйені құру процесінде қолданылатын қорғаныс құралдары да бар. Құпия ақпаратты қорғаудың барлық құралдары сертификатталған болуы керек [4].

2 Құпия ақпаратты қорғау құралдарын сертификаттау

Ақпараттық қауіпсіздік жүйесін ұйымдастыруда қолданылатын құпия ақпаратты қорғау құралдары мемлекеттік стандарттарға сәйкес сертификатталуы керек.

Сертификаттау - бұл қауіпсіздік өнімдерін мемлекеттік стандарттармен салыстыру және одан әрі сәтті тестілеу кезінде қолдануға рұқсат беру процесі [5].

Қауіпсіздік және ақпаратты қорғау талаптарына сәйкес ақпаратты қорғау құралдарын сертификаттау - мемлекеттік стандарттардың талаптарына сәйкес ақпаратты қорғаудың аппараттық және бағдарламалық құралдарының қасиеттерін растау жөніндегі ұйымдастырушылық шаралар. Қолданыстағы заңнама талаптарына сәйкес ақпаратты қорғау құралдары міндетті сертификаттауға жатады [6].

Мемлекеттік құпияны құрайтын мәліметтер. Мемлекеттік құпия - өзінің әскери, сыртқы саяси, экономикалық, барлау, қарсы барлау және жедел-іздестіру бағыттары саласындағы мемлекеттің қорғауындағы ақпарат. Мұндай мәліметтерді тарату Қазақстан Республикасының қауіпсіздігіне зиян тигізуі мүмкін.

Мемлекеттік ақпараттық ресурстар - мемлекет меншігіндегі ресурстар.

Жеке деректер - құпия ақпараттың тақырыбына тікелей немесе жанама қатысты кез келген ақпарат.

3 Ақпаратты қорғау әдістері мен құралдары

Ақпараттық қауіпсіздік құралдарын құрудың негізгі принциптері.

Ақпараттық қауіпсіздік құралдарын құрудың негізгі принциптері:

- ақпараттық қауіпсіздік жүйесін құрудың жүйелік тәсілі, бұл тәсіл бағдарламалық қамтамасыз ету, аппараттық, физикалық және басқа қорғаныс құралдарының оңтайлы үйлесімін қамтиды.

- жүйенің үздіксіз даму принципі. Бұл принцип ақпараттық қауіпсіздік жүйесін ұйымдастырудағы басты принциптердің бірі болып табылады. Құпия ақпаратты ұрлау әдістері үнемі дамып отырады, сондықтан ақпараттық жүйенің қауіпсіздігін қамтамасыз ету тұрақты бола алмайды. Бұл динамикалық процесс, ол қорғаныс жүйесін түрлендірудің ең ұтымды әдістері мен тәсілдерін талдаудан және жүзеге асырудан тұрады.

- қорғалатын ақпаратқа қол жеткізудің өкілеттіктерін бөлу және азайту.

- рұқсат етілмеген кіру әрекеттерін толық бақылау және тіркеу. Әрбір қолданушыны сәйкестендіру және аутентификациялау және оның әрекеттерін бақылау қажеттілігі, содан кейін мамандандырылған журналдарда әр түрлі әрекеттер фактілері атап өтіледі. Сондай-ақ, ақпараттық жүйеде алдын-ала тіркеусіз кез-келген әрекетті орындауға шектеу.

- қорғаныс жүйесінің сенімділігін қамтамасыз ету, яғни ақаулар, ұрының қасақана әрекеттері немесе жүйеде қолданушының қателіктері кезінде сенімділік деңгейін төмендетудің мүмкін еместігі.

- жүйенің дұрыс жұмысын бақылау.

- жүйені пайдаланудың экономикалық негіздемесін ұсыну. Бұл қауіп-қатерді жүзеге асыру кезінде құпия ақпаратқа рұқсат етілмеген қол жеткізуден болатын зиянның ақпараттық қауіпсіздік құралдарын әзірлеу мен пайдалану шығындарынан едәуір асып түсуімен көрінеді.

Осы принципптерге сүйене отырып, ақпараттық қауіпсіздік құралдарын құру өте ұзақ және еңбекқор процесс деген қорытынды жасауға болады. Жүйені жобалау және енгізу кезінде көптеген аспектілерді ескеру қажет. Бұл Қазақстан Республикасының заңнамасында көзделген құқықтық нормалар және жүйе жасалынатын кәсіпорынның экономикалық аспектілері.

Қорытындылай келе, Қазақстан Республикасының барлық заңнамалық актілерін қанағаттандыратын, жоғары сапалы ақпаратты қорғау жүйесін құру үшін тек сертификатталған ақпараттық қауіпсіздік құралдарын қолдану қажет.Ақпараттық қауіпсіздік объектісін егжей-тегжейлі талдау компанияның немесе ұйымның барлық осал жерлерін анықтау үшін қажет.

Ақпаратты қорғаудың ұйымдастырушылық құралдары.

Ақпаратты қорғаудың ұйымдастырушылық құралдарының кешенін әзірлеу қауіпсіздік қызметінің құзыретіне кіруі керек.

Көбінесе қауіпсіздік мамандары:

Компьютерлік техникамен және құпия ақпаратпен жұмыс істеу ережелерін белгілейтін ішкі құжаттаманы әзірлеу;

Жеке құрамға брифинг және мерзімді тексерулер жүргізу; жұмыстан белгілі болған ақпаратты жария еткені немесе дұрыс пайдаланбағандығы үшін жауапкершілікті көрсететін еңбек келісімшарттарына қосымша келісімдерге қол қою секілді жұмыстармен айналысады.

Маңызды мәліметтер жиынтығы қызметкерлердің біреуінің қарамағында болған жағдайларды болдырмау үшін жауапкершілік салаларын шектеу; жалпы жұмыс процесі бағдарламаларында жұмысты ұйымдастыру және маңызды файлдардың желілік дискілерден тыс сақталмауын қадағалау;

Деректерді кез-келген пайдаланушының, соның ішінде ұйымның жоғарғы басшылығының көшірмесінен немесе жойылуынан қорғайтын бағдарламалық өнімдерді енгізу;

Қандай да бір себептермен істен шыққан жағдайда жүйені қалпына келтіру жоспарларын жасау.

Егер компанияда арнайы ақпараттық қауіпсіздік қызметі болмаса, шешім кешенді қауіпсіздік ұйымдарын шақыру болып табылады. Қашықтағы қызметкер компанияның инфрақұрылымын тексеріп, оны сыртқы және ішкі қауіптерден қалай қорғауға болатындығы туралы ұсыныстар бере алады. Сондай-ақ, ақпараттық қауіпсіздіктегі ұйымдар ақпаратты қорғау үшін арнайы бағдарламаларды пайдалануды көздейді.

Ақпаратты қорғаудың техникалық құралдары

Ақпаратты қорғаудың техникалық құралдар тобы аппараттық және бағдарламалық жасақтаманы біріктіреді. Негізгі ұсыныстар:

Компьютерлік жүйеде маңызды мәліметтер жиынтығының сақтық көшірмесін жасау және қашықтықтан сақтау ;

Деректердің қауіпсіздігі үшін маңызды барлық желілік ішкі жүйелердің қайталануы және сақтық көшірмесі;

Жекелеген элементтер жұмыс істемеген жағдайда желілік ресурстарды қайта бөлу мүмкіндігін құру;

Резервтік қоректендіру жүйелерін пайдалану мүмкіндігін қамтамасыз ету;

Жабдықтың өрттен немесе судан зақымдануынан қауіпсіздікті қамтамасыз ету;

Мәліметтер базасын және басқа ақпараттарды рұқсатсыз қол жеткізуден қорғайтын бағдарламалық жасақтаманы орнату.

Техникалық шаралар кешеніне компьютерлік желілер объектілерінің физикалық қол жетімсіздігін қамтамасыз ету шаралары да кіреді, мысалы, бөлмені камералармен және дабылды құрылғылармен жабдықтау сияқты практикалық әдістер.

Аутентификация және идентификация

Ақпаратқа рұқсатсыз қол жеткізуді болдырмау үшін сәйкестендіру және аутентификация сияқты әдістер қолданылады.

Аутентификация - бұл пайдаланушының қабылданған сәйкестігін тексеру тәсілдерінің жүйесі.

Бұл деректерге қол жеткізуді қамтамасыз етуге немесе керісінше бас тартуға бағытталған. Түпнұсқалық, әдетте, үш жолмен анықталады: бағдарламамен, арнайы құрылғымен, адаммен. Бұл жағдайда аутентификацияның объектісі тек адам ғана емес, сонымен қатар техникалық құрылғы немесе мәліметтер бола алады.

4 Несиелік бюро мысалында ақпаратты кешенді техникалық қорғау

4.1 Ұйымдық құрылым

Кешенді қорғаныс жүйесінің дамуын жақсы түсіну үшін қорғаныс салынатын кәсіпорын болуы керек. Мысал ретінде несиелік бюроларды алайық.

Несиелік бюро - несиелік тарихты жасайтын, несиелік есептер беретін және басқа да қызметтерді ұсынатын ұйым. Осылайша, несиелік тарих бюросының негізгі міндеттерінің бірі несиелік мекемелер ұсынған ақпаратты қабылдау, өңдеу және сақтау болып табылады. Сонымен бірге, қауіпсіз арналар арқылы ақпарат беруді қамтамасыз ету қажет. Сондай-ақ, бюроның несиелік тарихының қауіпсіз сақталуын қамтамасыз ету қажет.

Бюроның қауіпсіздік саясатына сәйкес қорғау объектілері:

Коммерциялық құпияны құрайтын мәліметтер мен жеке деректерд және құпия ақпарат.

Құпия сипаттағы ақпараттың құрамы, оның мазмұны бюроның бас директоры бекіткен «Ұйымда өңделетін құпия сипаттағы ақпарат тізбесі» құжатында айқындалады.

Құпия ақпараты бар әр түрлі қол жетімділік деңгейіндегі несиелік тарих бюроларының ақпараттық ресурстары.

Несиелік тарих бюросының ақпаратты қорғау құралдарының конфигурациясының параметрлері.

4.2 Ақпараттық-коммуникациялық технологияларды қолдануға қойылатын талаптар

Несиелік бюроның ақпараттық жүйесі келесі талаптарға сәйкес келеді:

- техникалық тапсырма негізінде және кезеңдері мен тәртібін реттейтін несиелік бюроның ішкі құжаттарына сәйкес несиелік бюроның ақпараттық жүйесін (немесе дайын өнімді бейімдеу) әзірлеу, енгізу және өзгерту, тестілеу, қабылдау және пайдалануға енгізу, сондай-ақ барлық кезеңдерді құжаттау үшін;
- несиелік бюроның ақпараттық жүйесін пайдаланушыларға қол жеткізу құқығының сарапануын қамтамасыз ету;
- несиелік бюроның ақпараттық жүйесінің шоттарын басқаруды қамтамасыз ету;
- несиелік бюроның ақпараттық жүйесінің қорғалатын мәліметтерінің ақпараттық қауіпсіздігін қамтамасыз ету.

4.3 Ақпараттық қауіп моделін талдау

Ақпараттық қауіпсіздік жүйесін дамытудағы негізгі міндеттердің бірі - қауіп моделін құру. Бұл автоматтандырылған жүйенің әлсіз жақтарын

толығымен бағалауға мүмкіндік береді. Қауіпсіздік мақсаттары мен талаптары бағытталған қауіптердің негізгі топтары:

Несиелік тарих туралы ақпаратты қамтитын ақпаратпен рұқсат етілмеген қол жетімділікке байланысты қауіп-қатерлер, оны өңдеу және сақтау кезінде.

Несиелік тарих туралы ақпаратты (оның ішінде несиелік тарихтың мәліметтер базасын қоса алғанда) рұқсат етілмеген көшірумен (ұрлаумен) байланысты қауіптер.

Мүдделі тұлғаларға берілген несиелік тарихы туралы ақпараттың қол жетімділігінің бұзылуымен байланысты қауіптер.

Несиелік тарих туралы ақпаратты мамандандырылған бағдарламалық жасақтама мен жабдықты қолдана отырып, деректерді беру арналарына қатысты қауіптер.

Бағдарламалық және аппараттық құралдардың істен шығуына байланысты несиелік тарихы туралы ақпараттың жоғалуына байланысты қауіптер.

Несиелік тарихқа сұраныс жіберу фактісі мен несиелік есептерді алу фактісін жоққа шығарумен байланысты қауіптер.

Компьютерлік вирустар мен басқа да зиянды бағдарламаларға байланысты қауіптер.

Рұқсат етілмеген ақпараттық әрекеттерді жүзеге асырумен байланысты қауіптер (қызметтер үшін «қызмет көрсетуден бас тартуға», бағдарламалық жасақтама мен аппараттық құралдардың конфигурациясының деректерін өзгертуге, аутентификация ақпаратын таңдауға және т.б.)

Ақпаратты қорғау жүйесін құрудағы қауіп моделі - бұл таптырмас нәрсе. Бұл шара несиелік тарих бюроларының автоматтандырылған жүйесінің әлсіз тұстарын анықтап, мақсатты тиімді қою үшін қажет.

Мысалы, несиелік бюро үшін ақпараттық қауіпсіздік жүйесін жасауымыз керек. Ақпараттық қауіпсіздік жүйесі несиелік тарих бюросының келесі негізгі ерекшеліктерін қамтамасыз етуі керек:

Кесте 1- Бюроның интеграцияланған техникалық қорғау жүйесінің мүмкіндіктері

Несиелік бюрода кешенді қорғаудың мүмкіндіктері және міндеттері	Қажеттілік
Қатынау объектілері мен объектілерін сәйкестендіру және аутентификациялау	Бюроның қауіпсіздік жүйесіне кіруді бақылау үшін қажет
Қатынау объектілері мен объектілеріне қол жеткізуді басқару	Жеңіл саралау және белгілі бір материалдарға рұқсат беру үшін
Қауіпсіздік оқиғаларын тіркеу	Оқиғалар есебін енгізу және қолданыстағы жүйені одан әрі талдау үшін

Шабуылды болдырмау (алдын алу)	Уақытылы шешім мен қорғау үшін
Ақпараттық қауіпсіздікті бақылау	Жүйенің мүмкіндіктерін тиімді талдау үшін
Ақпараттың тұтастығы	Бюро міндеттерін толығымен орындау
Ақпараттың қол жетімділігі	Кеңсенің тиімді жұмысы және барлық функцияларды орындау үшін
Құралдарды, байланыс жүйелерін және деректердің жіберілуін қорғау	Рұқсат етілмеген бұзу немесе басқа ақпарат тарап кететін арналардың қауіптерін болдырмау немесе азайту

Кесте 2 - Бюроны жан-жақты қорғау жүйесіне қойылатын талаптар мен қызыметтер

Бюроны жан-жақты қорғау жүйесіне қойылатын талаптар	Атқаратын қызыметі
Қауіпсіз байланыс арналары	Құпия ақпаратты беру және қабылдау үшін қауіпсіз байланыс арналарын құру.
Қауіпсіз сақтау орны	Несиелік бюроларда құпия ақпаратты қауіпсіз сақтау.
Жүйелік бақылау	Несиелік тарих бюроларының автоматтандырылған жүйесінің қауіпсіздік деңгейінің мониторингі (бағдарламалық жасақтама функцияларын мезгіл-мезгіл тексеріп отыру, оларды мерзімді жаңарту және тиімділікті бақылау).
Сервер бөлмесі	Сервер үшін - құпия ақпараттың сақтық көшірмесі; жүйенің элементтері байланыс арнасы істен шыққан жағдайда оқиғалар туралы ақпараттың динамикалық сақтық көшірмесін жасау мүмкіндігі болуы керек.

4.4 Несиелік бюро үшін техникалық қорғаудың кешенді жүйесін енгізу

Электрондық құжат айналымын ұйымдастыру

Қазіргі уақытта электрондық құжат айналымын ұйымдастырудың екі нұсқасы бар:

Үшінші тұлғалардың көмегімен жүзеге асыру.

Өзіңіздің электрондық цифрлық қолтаңбаңызды қолдану арқылы жүзеге асыру.

Әрине, бірінші нұсқа неғұрлым ыңғайлы және үнемді, өйткені барлық негізгі функцияларды үшінші тарап ұйымы орындайды. Мәселен, электронды құжат айналымын жүзеге асыратын қызметтерді ұсынатын компаниялар бар, ал мамандандырылған бағдарламаларды сатып алу қажет емес, өйткені бұл компанияның өнімі кез-келген бухгалтерлік бағдарламамен үйлесімді. Бірақ, бұл қызметтер бухгалтерлік есептің электрондық құжат айналымын жүзеге асыруға бағытталғанын атап өткен жөн. Кез-келген басқа құжаттарды беру үшін мұндай қорғау құралдары жеткіліксіз болады. Оларды қарастырудың қажеті жоқ, өйткені әркімнің жұмысының мәні бірдей, кейде көмекші функциялар жиынтығы мен қызмет бағалары әртүрлі болады. Егер электронды құжат айналымын тек бухгалтерлік есеп жағдайында қарастыратын болсақ, онда мұндай шешім логикалық болар еді: қолданудың қарапайымдылығы, әртүрлі бухгалтерлік бағдарламалармен әмбебап үйлесімділік. Бірақ біздің жағдайда әртүрлі құжаттарды жіберу нұсқасын қарастыру қажет. Осылайша, біз үшінші тарап ұйымымен байланысты нұсқаны қарастыра алмаймыз.

Екінші нұсқа көп уақытты қажет етеді, өйткені сіз сертификатталған криптографиялық құралды, ЭЦҚ сертификатын өз бетіңізше сатып алып, оны қауіпсіздік жүйесіне қосасыз.

Құжаттарға қол қою автоматты түрде болу үшін қажет болғандықтан, несиелік бюроның автоматтандырылған жүйесіне кіретін бағдарламалық жасақтама қажет. Ол сонымен қатар кілттерді құру, цифрлық қолтаңбаларды құру және деректерді шифрлау функциясын қажет етеді. Мұндай құралды мәліметтер базасындағы деректерді шифрлауға қолдануға болады. Қажетті лицензиялар мен сертификаттарға ие цифрлық қолтаңбаларды шығаруға арналған құралдар нарығы айтарлықтай аз. Gamma Technologies-ті қарастырайық. Компанияда jacarta tumar деп аталатын өнім бар - алынбайтын жеке ЭСҚ кілтімен ЭСҚ құрудың жеке құралы, ол смарт-карта, usb, microusb таңбалауышы немесе securemicrosd картасы түрінде жасалған. Біздің жағдайда процессор тек берілген ақпараттың бүтіндігін қамтамасыз ету үшін қажет.

Несиелік тарих бюросы қызметкерлері үшін жеке электронды кілтті енгізу

Электрондық кілт - бұл бағдарламалық жасақтама мен құпия ақпаратты рұқсатсыз көшіруден, заңсыз пайдаланудан және рұқсатсыз таратудан қорғауға арналған аппараттық құрал.

Мұндай кілттерді пайдалану ұйым қызметкерлерінің жергілікті жұмыс компьютерлерінде және компанияның корпоративтік желісінде сәйкестендіру және аутентификация процестерін жақсартуға мүмкіндік береді. Өндірушілер екі негізгі нұсқаны ұсынады: смарт-карталар және usb кілттері. Біздің жүйе үшін usb кілттерін пайдалану ыңғайлы болады, өйткені оны жұмысшылардың компьютерлерінде пайдалану жоспарланған.

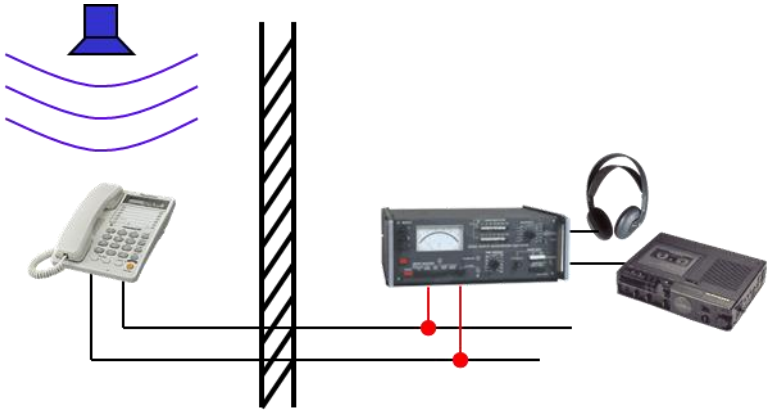
Электрондық кілттермен жұмыс кез-келген деңгейдегі пайдаланушылар үшін қиын емес. Кілттермен жұмыс істеу принципі келесідей: кілт компьютердің белгілі бір интерфейсіне бекітілген. Бұдан әрі қорғалған бағдарлама оны арнайы драйвер арқылы жібереді, ол бұрын көрсетілген алгоритмге сәйкес өңделеді және кері қайтарылады. Егер кілт дұрыс жауапты жіберсе, онда бағдарлама өз жұмысын жалғастырады. Әйтпесе, бағдарлама әзірлеуші көрсеткен әр түрлі әрекеттерді орындай алады.

Осылайша, мұндай кілттерді пайдалануға енгізу ақпараттық қауіпсіздік жүйесін құру кезінде қажетті шара болып табылады. Құпия сөзбен ғана аутентификация жеткіліксіз. 10-нан астам таңбадан тұратын құпия сөздің өзі оңай бұзылады, жұмыс компьютеріне кіре алады. Электрондық кілттің болуы ұрлардың жұмысын едәуір қиындатады.

4.5 Байланыс каналдары арқылы ақпараттың тарап кетуден қорғаудың техникалық құралдарын енгізу

Әдетте, көптеген ұйымдарда байланыс арналары (телефон және жергілікті желілер) арқылы ақпараттың тарап кету арналарына назар аударылмайды. Көптеген басшылар бұған уақыт пен ақша жұмсаудың қажеті жоқ деп санайды. Алайда, тәжірибелі ұрылар үшін барлық қажетті деректерді, мысалы, телефон желісін пайдалану арқылы алу қиын болмайды. Сондықтан байланыс арналарын қорғау ақпаратты қорғау жүйесін құру кезіндегі басым міндеттердің бірі болып табылады.

Сурет 1 – Ақпараттың байланыс каналдары арқылы таралу кезіндегі тарап кету арнасының сызбасы

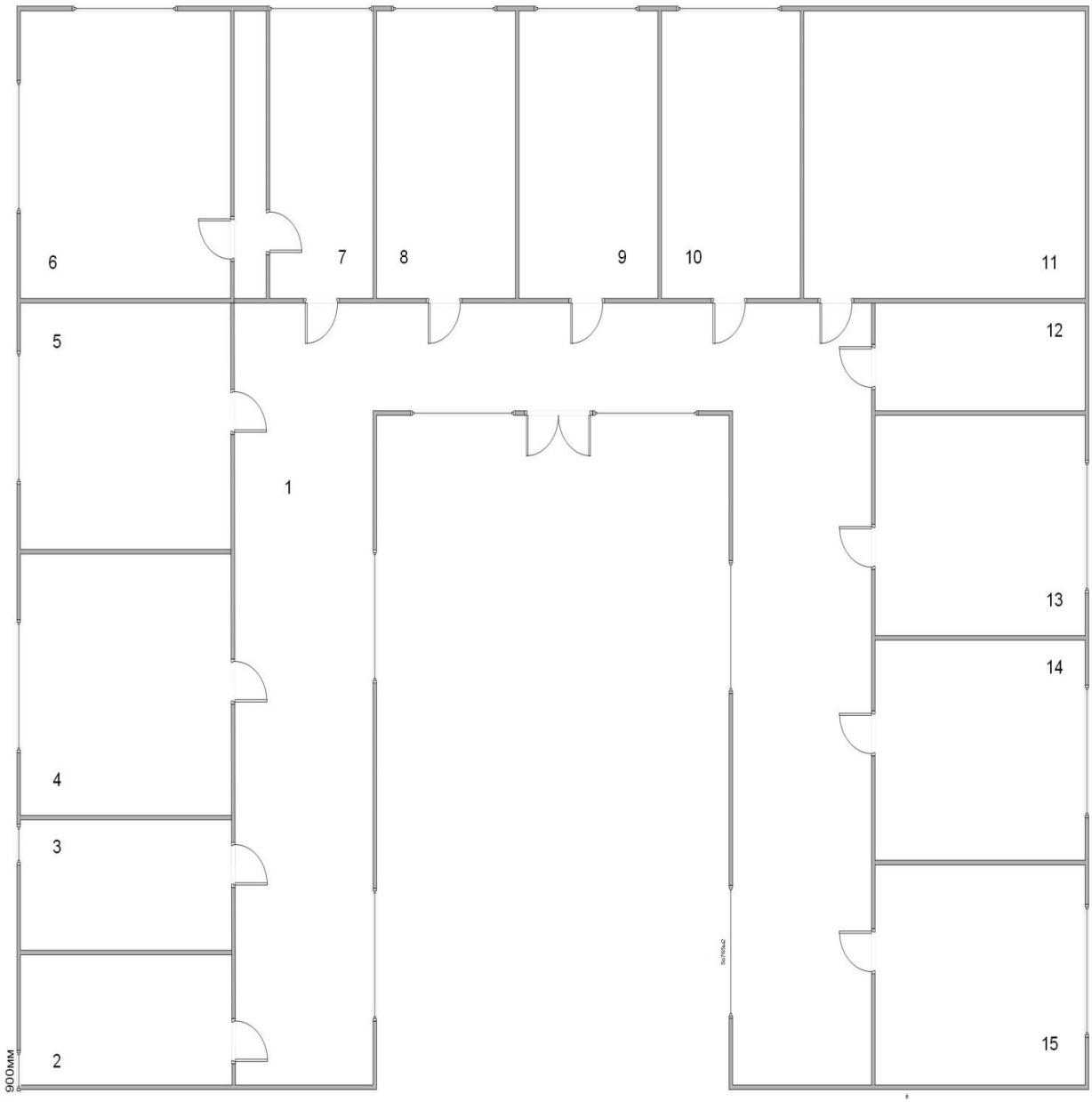


Сурет 2 –Акустоэлектрлік ақпарат тарау арнасы

Жұмысты және мақсатты жақсы түсіну үшін біз бірнеше бөлмелі кеңсенің үлгісін саламыз. Қызметтік паспорт:

Кесте 3 - Кеңсенің паспорты

Нөмір	Атауы	Аудан
1	Дәліз	160 м2
2	Кабинет №1	17 м2
3	Кабинет №2	17 м2
4	Кабинет №3	34 м2
5	Кабинет №4	32 м2
6	Директор кабинеті	38 м2
7	Хатшы кабинеті	19 м2
8	Бухгалтерлік есеп бөлімі	25 м2
9	Кабинет №5	25 м2
10	Кабинет №6	25 м2
11	Кездесу бөлмесі	51 м2
12	Сервер	14 м2
13	Кабинет №7	29 м2
14	Кабинет №8	29 м2
15	Кабинет №9	29 м2



Сурет 3 – Бас кеңсенің сызбасы

Телефон желілерін қорғау

Телефон желілеріндегі хакерлік шабуылдардан қорғауды қамтамасыз ететін негізгі техникалық құралдар кеңсе аралық экрандар болып табылады. Осындай құрылғылардың жұмыс істеу принципі: құрылғы компанияның автоматты телефон станциясымен қосатын цифрлық желілердің үзілісіне қосылған, пайдаланушылар мен қызмет көрсету арналарында фазалар кезінде болатын барлық оқиғаларды тұрақты бақылауды қамтамасыз етеді .

Сонымен қатар телефон блокаторлары бар. Олардың негізгі қызметі - параллель сызық арқылы тыңдау әрекеттерін бақылау және алдын алу.

Телефон желісі анализаторларын екі түрге бөлуге болады: жеке және тест жинақтары. Жеке дабылды алдын-ала тексерілген желіге орнату керек. Олар

телефон жұбының параметрлерін басқаруға қызмет етеді. Әдетте, мұндай дабылды «телефон күзетшілері» деп атайды. Мұндай күзет әдетте екі жарықдиодты розетка түрінде ұсынылады.

«Арна айқын», қызыл «Дабыл! Арна параметрлері өзгерді. « Мұндай жеке дабылдардың күмәнсіз артықшылығы - бұл жұмыстың қарапайымдылығы, кемшілігі - жалған дабылдың пайда болу ықтималдығы жоғары.

Тест жиынтықтары мамандардың сызықты тексеруіне арналған. Мұндай жинақ сызыққа зондтау сигналын жібереді және жауап сигналын талдайды, оның көмегімен кез-келген радиоэлементтердің қатарында ақпараттық қабылдау және тарату тізбектеріне тән болуын анықтайды.

«Ең жақсы қорғаныс - бұл шабуыл» - бұл телефон желілерін белсенді қорғауға арналған құрылғыларда қолданылатын қағида. Оларды әдетте телефон байланыстырушы деп атайды. Мұндай құрылғы жоғарғы дыбыстық диапазонда шуды қамтамасыз етеді, осылайша құрылғылардың кірісіндегі сигналдың шуылға қатынасын нашарлатады. Іс жүзінде, шуды басатын адам өте қатты дыбыс шығарады, оны айту мүмкін емес.

Анализаторлардың, супрессорлардың және блокаторлардың артықшылығы телефон желілерін қорғауға арналған әмбебап құрылғыларды үйлесімді түрде біріктіреді. Олар екі режимде жұмыс істейді: анықтау және басу. Желіге кез-келген байланыс байланысы кезінде құрылғы сізге дабыл береді, содан кейін сіз сөндіру режимін қосуға болады. Желіге түсетін кедергі құрылғыдан автоматты телефон станциясына дейінгі бөлікке әсер етеді, осылайша жоюдың барлық құралдарын жұмыс істемейтін жағдайға жеткізеді.

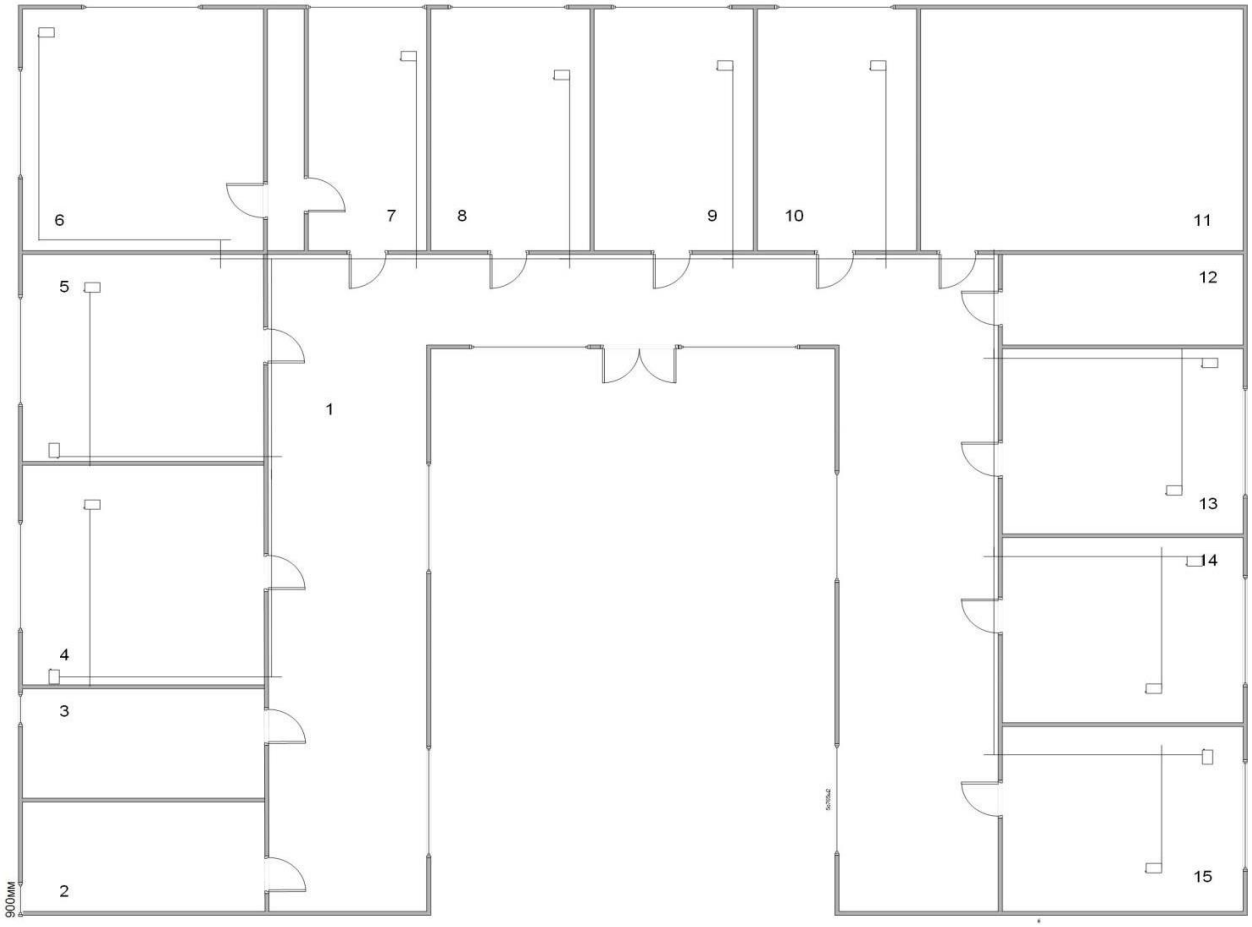
Ақпаратты қорғаудың бұл класы телефон желілері арқылы тарап кетуден, телефон желілері арқылы сөйлесулердің қорғалуын қамтамасыз ету үшін ең қолайлы болып табылады.

Жергілікті желіні қорғау

Дербес компьютерде жұмыс істеуден жалпы корпоративті желіде жұмыс істеуге көшу кезінде желілерде ақпаратты қорғауды қамтамасыз етуді едәуір қиындатады. Бір компьютерді бұзу жеткілікті, өйткені бүкіл желінің ресурстары ашық болады.

Жергілікті желіні қорғауды ұйымдастыру кезінде ең бірінші кезекте қызметкерлердің әртүрлі санаттарына қол жетімділікті бөлу керек. Бұл жағдайда ұйымның жергілікті желісіне ену қаупі айтарлықтай аз болады. Әрине, қол жетімділікті басқару жеткіліксіз. Техникалық құралдарға жүгіну керек. Жергілікті желінің қауіпсіздігін қамтамасыз етудің ең кең таралған құралы - кернеуді қорғаушылар.

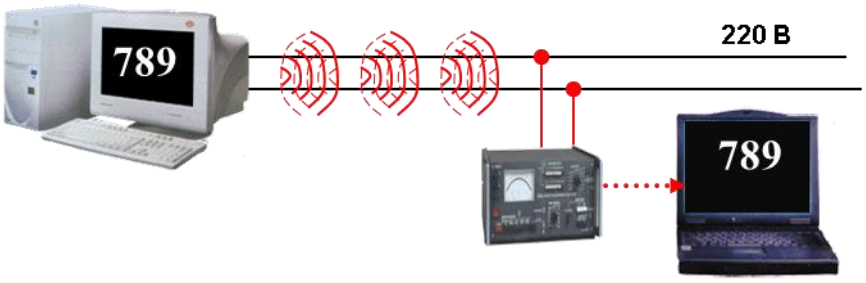
Компьютерлердің жергілікті байланыс желілері бар кеңсенің моделін құрайық:



Сурет 3.1 – Компьютерлік желі

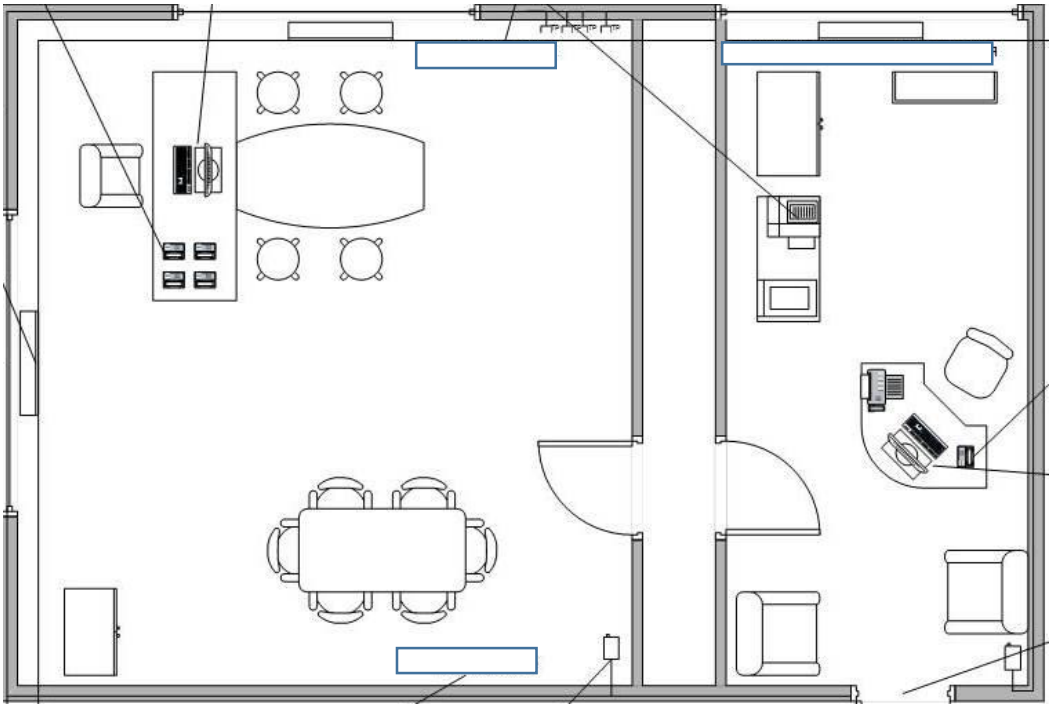
Кесте 4 – Компьютерлер саны

Бөлме	Компьютерлер саны, дана.
1	0
2	0
3	0
4	2
5	2
6	1
7	1
8	1
9	1
10	1
11	0
12	0
13	2
14	2
15	2



Сурет 4 – Компьютерде өңделген ақпараттың тарап кетуінің параметрлік арнасы

Біздің несиелік бюроның ықтимал қауіп түрлерін қарастырайық.



Сурет 5 – Директор / хатшы кеңсесі

Кесте 5 – Қауіптердің түрлері мен көздері

Қауіп түрі	Құрылғылар
Жоғары жиілікті енгізу	Телефон жиынтықтары
Акустикалық	Желдету, ашық есік, терезе
Акустоэлектрлік	Телефондар, электрмен жабдықтау
Ақпараттың тарап кету арнасы жалған электромагниттік сәулелену	Компьютерлер
Акустикалық-оптикалық	Жабық терезе
Виброакустикалық	Қабырға, құбырлар

Ақпараттың басқа арналары	Ұялы телефондар, диктофондар, арнайы құрылғылар. техникалық құралдар

Ақпараттың ағып кету қаупі мен шығындарынан қорғалатын жабдықты таңдау. Біздің кешенге қажетті жабдықтың шамамен құнын есептейік:

Кесте 6 – Қорғаныс жабдығы және құны

Қорғаныс құралдары	Құны теңгеде
Эгида груп тобының қауіпсіздігі мен өртке қарсы дабылы	60 000
8 1MP камераларға арналған Dahua HD бейнебақылау жинағы	122 000
Биометриялық уақытқа келу және кіруді бақылау терминалы ANVIZ W1-PRO	63 900
Жүйе виброакустикалық шу akip-3501/2 - шу генераторы	994 000
Төмен токты қорғаныс құрылғысы (мп-1а, 4,5)	12 000
Жүйе шу сигналдар пами (гш-1000, Гном-3м)	480 000
КриптоПро JCP	120 000
ОР-230 Желілік кедергілерді басу сүзгісі	28350

Қажетті жабдықтың жалпы құны (монтаждау жұмыстарын қоспағанда) 1 880 250 теңгені құрайды.

Қорытынды

Бұл жоба нысанды кешенді техникалық қорғау жүйесін жасау мақсатында жасалды.

Осы дипломдық жобаны іске асыру барысында қолда бар ақпараттық қауіпсіздік құралдарына талдау жүргізілді. Келесі қасиеттерге ие несиелік тарих бюросы мысалында ақпараттық қауіпсіздік жүйесінің мысалы келтірілген:

Құпия ақпаратты сенімді сақтау үшін мәліметтер базасын шифрлау.

Берілген ақпараттың тұтастығы мен өзгермейтіндігін қамтамасыз ету үшін ЭЦҚ қолдану.

Жұмыс орнындағы объектілерді сәйкестендіру мен аутентификациялаудың неғұрлым сенімді процедурасы үшін әр қызметкер үшін жеке электронды кілтті қолдану.

Ақпаратты телефон желілері арқылы жоюға қарсы құралдарды қолдану.

Ақпаратты жергілікті желі арқылы жоюға, сондай-ақ компанияның корпоративтік желісіне рұқсатсыз кіруге қарсы құралдарды қолдану.

Пайдаланылған әдебиеттер тізімі

1 СТ РК 34.025-2006 Қорғалатын дизайндағы автоматтандырылған жүйелерді құру тәртібі

2 СТ РК 34.012-2002 Ақпараттық технологиясы. Бағдарламалық жасақтаманы сертификаттау. Бағдарламалық құжаттаманың сапасын бағалаудың типтік әдістемесі

3 Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – 96 б.

4 Аверченков В.И. Организационная защита информации: учеб. Пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 184 с.

5 Белкин П.Ю. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учеб. пособие для вузов/ П.Ю. Белкин, О.О. Михальский, А.С. Першаков. – М.: Радио связь, 2000.-215 с.

6 Способы предотвращения утечки информации электронндық нұсқа https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/

7 Утечка информации по каналам пэми и способы их защиты электрондық нұсқа https://www.applied-research.ru/ru/article/view?id=10110

8 Джонс К.Д., Шема М., Джонсон Б.С., Инструментальные средства обеспечения безопасности/К.Д. Джонс, М. Шема, Б.С. Джонсон.- ИНТУИТ, 2007.-1028 с.

9 Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1.Технические каналы утечки информации: учеб. пособие. – М.: Гостехкомиссия РФ, 1998. – 320 с.

10 Хорев А.А. Методы и средства поиска электронных устройств перехвата информации: монография. – М.: МО РФ, 1998. – 224 с.

11 Исаев А.Б. Современные технические методы и средства защиты информации Учеб. пособие. М.: РУДН, 2008. – 253 с.

12 Хорев А.А. Методы выявления электронных устройств перехвата информации, подключаемых к проводным коммуникациям// Специальная техника. – М.: 2016. – № 2 – С. 48 – 63. (1,03 п.л.) (ВАК)

ҒЫЛЫМИ ЖЕТЕКШІНІҢ

ПІКІРІ

Есен Жалғас Айдынұлы
(студенттің Т.А.Ә.)
5В100200 Ақпараттық қауіпсіздік жүйелері
(мамандықтың шифрі және атауы)
дипломдық жобасына
(жұмыс түрінің атауы)

Тақырыбы: Ақпараттандыру объектісін кешенді техникалық қорғау жүйесін әзірлеу

Ақапараттық қауіпсіздіктің заманауи қауіп-қатерлеріне қарсы тұру және жекеше алғанда киберқылмыспен күресу қажеттігін алдын-ала болжай келе, Елбасы «Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» Қазақстан халқына жолдауында «Қазақстан киберқалқаны» жүйесін қалыптастыруды тапсырды.

Осыған байланысты Ж.А. Есен бүгінгі таңда өзекті тақырыптардың бірін «Ақпараттандыру объектісін кешенді техникалық қорғау жүйесін әзірлеу таңдады». Дипломдық жобасында автор заманауи қорғау жүйелерін зерттеп, оларға баға бере алды, ақпарат таралуының арналарына шолу жасады. Сонымен қатар, өз жұмысында мысалы ретінде несиелік бюро бөлмелерін кешенді техникалық қорғау жобасын әзірледі.

Студент дипломдық жобада міндеттерді толығымен орындады. Осыған байланысты, Ж.А. Есен дипломдық жобасын орындау мәселесіне толық жауапкершілікпен қарағандығы даусыз.

Жұмыс барысында Ж.А. Есен шығармашылық, тапқырлық пен тәуелсіздік көрсетті. Ғылыми жетекшінің ескертулері мен нұсқауларына дұрыс және уақытында жауап берді, белгіленген кемшіліктерді сапалы түрде түзетіп отырды.

Жоғарыда баяндалғандарды ескере отырып, Есен Жалғас Айдынұлының дипломдық жобасы аяқталған тәуелсіз зерттеу болып табылады және оны қорғауға ұсынуға болады деп санаймын.

Ғылыми жетекші
сениор-лектор, магистр
(лауазымы, ғылыми дәрежесі, атағы)
Батыргалиев А.Б.
(қолы)

2021 жылғы «31» мамыр

Протокол анализа Отчета подобия заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Есен Ж.А.
Название: Разработка системы комплексной технической защиты объекта
Координатор: Батыргалиев А.Б.
Коэффициент подобия 1: 4,26
Коэффициент подобия 2: 2,60
Замена букв:0
Интервалы:0
Микропробелы:2
Белые знаки:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

……
……
Заимствования добросовестные
……
……

Дата «02» 06 2021 г. Сейлова Н.А. , подпись зав.кафедрой

Протокол анализа Отчета подобия Научным руководителем

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Есен Ж.А.
Название: Разработка системы комплексной технической защиты объекта
Координатор: Батыргалиев А.Б.
Коэффициент подобия 1: 4,26
Коэффициент подобия 2: 2,60
Замена букв:0
Интервалы:0
Микропробелы:2
Белые знаки:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

……
…
……
…
Заимствования добросовестные
……
……
…

Дата «31» мая 2021г. _____ Подпись Научного Руководителя