ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Электронды поштаны пайдалану кезінде ақпаратты қорғау»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Нурлан Арайлым Тобы: СИБк-15-1
Ғылыми жетекші: проф. Ахметов Б.С.

Кеңесшілер:
Экономикалық бөлім бойынша:
э.ғ.к., профессор Аренбаева Қ.Г.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
аға оқытушы Торғаев Д.Д.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «31» 05 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
проф. Ахметов Б.С.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «6» 06 2019 ж.
(қолы)

Мөлшер бақылаушы:
аға оқытушы Лекарова Л.Б.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «8» маусым 2019 ж.
(қолы)

Пікір беруші:
т.ғ.к., ассистент-профессор Сейлова И.А.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «07» 06 2019 ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5B100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Нұрлан Арайлым Айдынқызы
(аты-жөні)

Жобаның тақырыбы: Электронды поштаны пайдалану кезінде ақпаратты қорғау

2018 ж. «26» 10 № 124 университтет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «12» 06 2019 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Пошта серверінің қорғау мәселелері, электронды пошта сервистеріне ықтимал қауіп-қатерлер және қорғаныс құралдары қарастырылды. Электрондық поштаны пайдалану ерекшеліктері, бейінген шифрлау арқылы пошта трафигін өткізудің негізгі принциптері сипатталған.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны: Пошта сервері инфрақұрылымындағы орны, оның атқаратын рөлі, пошта өтетін ерекшелерін талдау. Нерілікті келі инфрақұрылымын құрылымын талдап отырып, оған тіркелетін поштаның шифрын орнатылған қолдану.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі: Бұғат айналып жолы
Поштаның желідегі ашық түрі
Поштаның шлюздан өту кезеңдері
Пошта трафигінің өтетін жолы
Пошта серверінің шлюзбен жұмысы

Негізгі ұсынылатын әдебиеттер: 1 Прохода А.Н. Обеспечение интернет-безопасности.
2 Тарасов А., Смлов О. Безопасность систем электронной почты.
3 Блан Р. Администрирование почтовых серверов Sendmail.
4 Кузьминкова О., Анализ рынка программных средств защиты компьютерных систем

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Экономика бөлімі	Арепбаева Ж.Г.	04.03-31.05.18	
Өміртіршілік қауіпсіздік бөлімі	Торғаев Э.Э	20.05-31.05	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Кіріспе	2.02.2019	
Қорғау объектісі туралы жалпы мәліметтер.	4.03-2019	
Электронды хат алмасу және электрондық пошта сервистеріне кіретін қауіп-қатерлерді шолу.	12.03.2019	
Электрондық пошта қызметінің негізгі принциптері.	15.03.2019	
Электрондық хат алмасу, электрондық пошта сервистеріне қауіп-қатерлерді қорғау әдістерін шолу.	21.03.2019 22.03.2019	
Прокси пошта шлюзі дегеніміз не?	1.04.2019	
Ерекшеліктері.	4.04.2019	
Вирустарды табу	1.04.2019	
Бағдарлама қызметі.	4.04.2019	
Техникалық-экономикалық негіздеме	26.04.2019	
Өндірістік қауіпсіздік.	26.04.2019	
Қорытынды	30.04.2019	

Тапсырманың берілген уақыты «2» 04 2019ж.

Кафедра меңгерушісі _____ (_____)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (Ахметов Б.С.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Нұрсаи А.А.)
(қолы) (аты-жөні)

АҢДАТПА

Дипломдық жоба тақырыбы: "Электрондық поштаны пайдалану кезінде ақпаратты қорғау". Талдау бөлімінде зерттелетін қорғау объектісі сипатталған, осы объектіге қатысты қарастырылып отырған тақырыптың өзектілігі көрсетілген, электрондық пошта сервистеріне ықтимал қауіп-қатерлер қарастырылды. Осы жобаның теориялық бөлімінде электрондық поштаның жұмыс принциптері қарастырылды және пошта хаттамаларының сипаттамасы берілді,электрондық хат жазысуға қауіп төндіруден қорғау әдістері қарастырылды. Практикалық бөлімде желілерде электрондық поштаны пайдалану ерекшеліктері, бөлінген шлюз арқылы пошта трафигін өткізудің негізгі принциптері сипатталған. Электрондық поштаны әртүрлі қауіптерден қорғаудың бағдарламалық құралдарының тиімділігін бағалау критерийлері бөлінді.

АННОТАЦИЯ

К дипломному проекту на тему: “Защита информации при использовании электронной почты”. В аналитической части описан исследуемый объект защиты, показана актуальность рассматриваемой темы применительно к данному объекту, рассмотрены возможные угрозы сервисам электронной почты. В теоретической части данного проекта рассмотрены принципы работы электронной почты и дано описание почтовых протоколов, рассмотрены методы защиты от угроз электронной переписке. Выделены критерии оценки эффективности программных средств защиты электронной почты от различных угроз.

ABSTRACT

To the diploma project on the topic: "Protection of information while using e-mail”. The analytical part describes the object of protection, shows the relevance of the topic in relation to this object, considers possible threats to e-mail services. In the theoretical part of this project, the principles of e-mail and a description of mail protocols, methods of protection against threats to e-mail. The criteria for evaluating the effectiveness of software to protect e-mail from various threats.

Мазмұны

Кіріспе

Бүгін электрондық пошта туралы естімейтін адамды табу өте қиын. Электрондық пошта-корпоративтік желілерде де, ғаламторда да кең қолданылатын қызмет түрлерінің бірі. Электрондық пошта арқылы жіберілген хабарлама бірнеше мың километр қашықтықта болса да, адресатқа санаулы минуттарда келеді. Соңғы жылдары интернеттің дамуымен электрондық пошта қызметі айтарлықтай өзгерді. Ол ұйым ішіндегі байланысты қамтамасыз ету құралы ғана емес. Бүгін электрондық пошта әр түрлі компаниялардан, елдер мен аймақтардан адамдарды біріктіреді және коммуникацияның, ақпаратты тарату мен бизнестегі түрлі үдерістерді басқарудың маңызды құралы болып табылады:

- жеделдік және пайдалану жеңілдігі;
- кез келген жерде дерлік қолжетімділік;
- хаттар мен салымдар форматтарының әмбебаптығы;
- сервистің арзандығы;
- жеткізу инфрақұрылымының сенімділігі мен жылдамдығы;
- электрондық поштаны өңдеу үшін қолданбалы арнайы бағдарламалық қамтамасыз етуді пайдалану.

Бірақ осы артықшылықтарға қарамас оны пайдалануға байланыстынегізгі тәуекелдер туындайды. Мысалы, электрондық поштаныңқолжетімділігі пайдаланушылар спамды тарату үшін поштаны қолдана бастағанда, пайдалану жеңілдігі және бақылаусыз ақпараттың, құжаттардың түрлі форматтарын жіберу мүмкіндігі - вирустар мен т.б. таралуына әкеледі. Осыған байланысты электрондық поштаны пайдалану кезінде ақпараттық қауіпсіздікті қамтамасыз ету жеке пайдаланушылар үшін де, ұйымдар үшін де аса өзекті міндет болып табылады.

Бұл жұмыстың мақсаты жергілікті есептеу желісінде электрондық поштаны пайдалану кезінде ақпараттық қауіпсіздікті қамтамасыз ету құралдарының параметрлерін таңдау және анықтау болып табылады. Қойылған мақсатқа жету үшін келесі негізгі міндеттер шешілетін болады:

- қорғау нысанының сипаттамасы;
- электрондық пошта жұмысының негізгі принциптері мен ерекшеліктерін шолу және талдау;
- электрондық пошта қауіп-қатерлерін және олардан қорғау әдістерін шолу;
- қауіпсіздіктің криптографиялық механизмдерін зерттеу;
- ашық кілттер архитектурасы технологиясының негіздерін зерттеу;
- ақпараттық қауіпсіздік және электрондық хат алмасу саласындағы нормативтік-құқықтық базаны шолу және талдау;
- электрондық поштаны қорғау құралдарын шолу және салыстырмалы талдау;

– ең қолайлы электрондық поштаны қорғау бағдарламалық құралын таңдау;

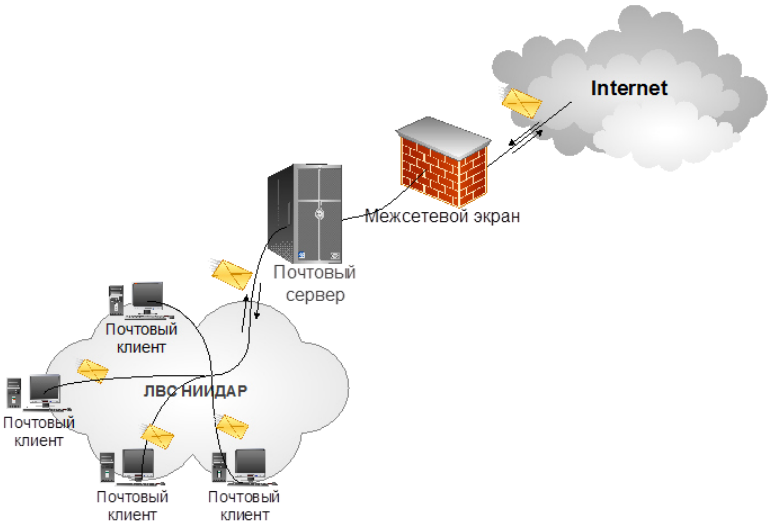
– ЛВС-да электрондық поштаны қорғауды қамтамасыз ету бойынша практикалық ұсыныстар әзірлеу ;

– таңдалған қорғаныс құралдарының тиімділігін бағалау.

1 АНАЛИТИКАЛЫҚ БӨЛІМ

1.1 Қорғау объектісі туралы жалпы мәліметтер

1.1 суреттегі электрондық пошта сервистері, электрондық хат алмасу, тиісінше оған қатысатын ақпарат түрлі қауіптерге ұшырайды. Оларды толығырақ қарастырайық.



Сурет 1.1 – Пошта жүретін трафик

1.2Электрондық хат алмасу және электрондық пошта сервистеріне ықтимал қауіп-қатерлерді шолу

Пошта қызметімен жұмыс кезінде интернет пайдаланушының келесі қауіптерді қорғайды:

- құпиялылық қатері;
- аутентификация қаупі;
- хабарлама тұтастығының қатері;
- бас тарту қатері;
- зиянды бағдарламаларды енгізу;
- спам.

Қауіптердің негізгі түрлерінен басқа қосымша – ақпаратты жоғалту, яғни маңызды ақпаратты кездейсоқ жою және ұйымның іскерлік беделіне зиян келтіру бар.

1) Құпиялылық қаупі.

Бұл қатерлерді егжей-тегжейлі қарастырайық. Бұл қауіп пошта хабарламаларының құпиялылығын ашу болып табылады. Сыртқы корреспонденттермен хат алмасу электрондық пошта ерекшелігіне байланысты үлкен қауіп төндіреді, хаттарды жіберу бағытын бақылау, сондай-ақ оларды көшіру және қайта бағыттау, жіберушінің/алушының аутентификациясын жүзеге асыру, хаттарды жібергеннен кейін қайтару мүмкін болмауы. Сонымен қатар, жіберілетін хат көшірмелерінің санын бақылау мүмкін емес немесе қиын. Электрондық хаттардың тақырыптары мен

мазмұны жиі ашық түрде жіберілетіндіктен, хабар мазмұнын Интернет арқылы жіберу барысында оқып, желі тораптарында ұстап қалуы мүмкін.

Қауіпті пайдаланушы аты мен POP-сервердің (немесе IMAP-сервердің) тіркелгісінің паролін ашық түрде ұстап тұрады. Бұл ақпаратты желілік талдаудың көптеген бағдарламаларының бірі арқылы ұстап алған қаскүнем пайдаланушының хаттарымен кез-келген нәрсені жасай алады: оқу, серверден жою, ал егер SMTP және POP серверлері біріктірілген болса, онда сіздің атыңыздан өз хаттарыңызды жіберу.

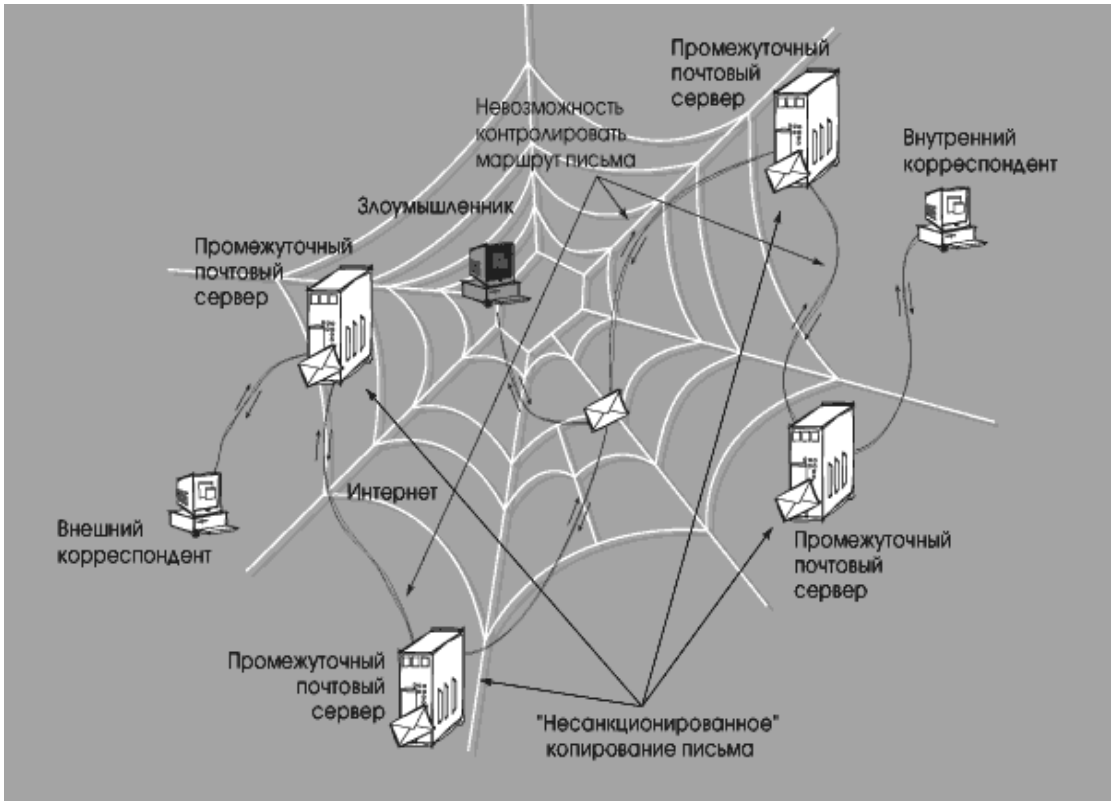
Электрондық поштаның ерекшеліктеріне байланысты тағы бір мәселе бар-электрондық пошта мұрағаттардағы ақпараттың бақылаусыз жиналуына мүмкіндік береді және іс жүзінде тиімсіз. Электрондық поштаны жою оңай емес. Хабарлардың резервтік көшірмелері жіберуші мен алушының дербес компьютерлерінде немесе олар жұмыс істейтін компаниялар желісінде қалуы мүмкін. Егер электрондық пошта хабары коммерциялық қызмет арқылы немесе интернет арқылы жіберілсе, онда ол бірнеше түрлі серверлер арқылы берілетін болады. Жіберуші мен алушы арасындағы тізбектегі әрбір сервер хабарламаның көшірмесін өз мұрағаттарында сақтай алады. Электрондық хаттың әрбір көшірмесінің орналасқан жерін әрі қарай жою арқылы анықтау тіпті компьютердің немесе сервердің қатты дискісінде хабарламаның қалмағанына ешқандай кепілдік бермейді. Кең қол жетімді бағдарламалық жасақтаманың көмегімен, тіпті қатардағы пайдаланушы электрондық пошта хабарын жойғаннан кейін қалпына келтіре алады.

Корпоративтік поштаға қатысты барлық осы ерекшеліктер, сондай-ақ электрондық хабарламаны көшірудің қарапайымдылығы және осы операцияны бақылаудың мүмкін еместігі қызметкердің корпоративтік ақпаратты компанияның ішіндегі және одан тыс жерлердегі кез келген адам санына жасырын және тиісті рұқсатсыз, бірден немесе қандай да бір уақыт өткеннен кейін бере алатынын ескеру қажет. Бұл ретте мұндай ақпарат компанияның қызметтік ақпаратын (шарттардың мәтіндерін, жоспарланған мәмілелер туралы мәліметтерді және т.б.), парольдерді, жүйелік деректерді, бағдарламалардың бастапқы кодтарын немесе басқа да құпия ақпаратты білдіруі мүмкін. Бұл, сайып келгенде, құпиялылықты елеулі бұзу қаупі бар және компания үшін жағымсыз салдарларға әкелуі мүмкін. Құпия ақпараттың шығуы-корпоративтік электрондық поштаны пайдаланумен байланысты маңызды қауіптердің бірі.

Қағаз хат-хабардан айырмашылығы, электрондық поштаны дұрыс емес мекенжайға жіберу өте оңай. Мұның себебі мекенжай кітаптарын дұрыс пайдаланбау, сондай-ақ алушының мекен-жайын көрсетудегі қате немесе одан да нашар, хабар пайдаланушылардың үлкен тобына хабарды таратуды көздейтін опцияны кездейсоқ таңдау болуы мүмкін, ал Хабар құпия болып табылады.

1.2 суретте сипатталған компания қызметкерлері кәсіпорынға зиян келтіру мақсатында немесе жай ғана абайсызда өз пайдасын алу мақсатында жабық сипаттағы ақпаратты қамтитын хаттарды жібере алады, өйткені қандай

ақпаратты жіберуге болатынын білмеуі мүмкін, ал қандай да болмасын мүмкін емес.



Сурет 1.2 – Құжат айналымы желісі

Сондай-ақ құпиялылық қатерлеріне компания қызметкерлерінің жеке пайдасы немесе абайсызда құпия ақпаратты электрондық пошта арқылы жіберуін жатқызуға болады.

2) Аутентификация қаупі.

Дәлме-дәлдігі-деректерді (аутентичность) өңдеуде - деректердің шынайы болу қасиеті, бұл деректердің ақпараттық процестің заңды қатысушылары құрылғанын білдіреді. Қауіптің осы түрінің мысалы - "маскарад" - жалған хаттарды тарату. Пошта серверінің хабарламалары мәтіндік түрде дайындалады және кейбір тәжірибе болған жағдайда жіберушінің нақты пошталық мекенжайы компрометацияланатын адамның мекен-жайымен ауыстырылатын пошта Жолдауын жасау қиын емес. Шынайы авторды анықтау үшін хабардың тақырыптарына хабарласу қажет, бұл адам үшін өте қиын.

3)Хабарламалардың тұтастық қатері.

Бүтіндік қаупі почта хабарламаларын кездейсоқ немесе әдейі түрлендіру, бұрмалау немесе оларды ауыстыру болып табылады.

4)Бас тарту қаупі.

Бас тарту қаупі құжат авторы оны жасаудан және (немесе) таратудан бас тартқан кезде туындайды

5)Зиянды бағдарламаларды енгізу.

Қауіп-қатердің бұл түрі netbus немесе Back Orifice типті вирустар немесе "трояндық аттар" болуы мүмкін бағдарламалар файлдарының хаттарына салымдарға қатысты. Бұл қолданбаларды ашу деректердің жоғалуына немесе компьютер қызметінің проблемаларына әкелуі мүмкін. Мұндай бағдарламаларды енгізудің басқа нұсқасы жаңартуларды жүктеу үшін хат жіберушінің ұсынған "пайдалы" сілтемелерді, мысалы Web-браузерді немесе электрондық коммерция бағдарламаларын тарату болып табылады, ол бойынша пайдаланушы қаскүнемдің сайтына кіреді. Сондай-ақ адрестік кітаптар арқылы таратылатын вирустар да бар: клиенттік компьютерлердің бірінде іске қосылған вирус пошталық клиенттің адрестік кітабын қарап, өзін табылған мекенжайлар бойынша өзі жібереді.

Пошта клиенттерін қорғау кемшіліктерін пайдаланатын пайдаланушының компьютерінде зиянды бағдарламаны іске қосудың тағы бір жолы бар: пошта клиентінің диалогында хабардың өзін ашу компьютерде зиянды бағдарламаны жүктеу және іске қосу үшін жеткілікті.

6)Спам.

Әдетте, бұл әртүрлі қызметтердің, тауарлардың және т.б. ұсыныстарын қамтитын хаттар. Қажетсіз поштаның көп саны арналарды жүктейді, пошта жәшіктерін" өшіреді", қажетсіз хаттарды жою уақытын алып тастайды және қажетсіз хаттарды кездейсоқ жою мүмкіндігін арттырады. Әрине, тарату, мысалы, жарнамалық сипаттағы хабарламаларды тікелей ұйымның пошта жүйесін "ластау" мақсатын көздемейді, алайда жанама кері салдарларға әкеледі. Бір корпоративтік желінің барлық пайдаланушылары кіре алатын тарату тізімін пайдалану және осы пайдаланушылардың бір мезгілде жарнамалық сипаттағы хабарламаларды алуы компанияның желілік ресурстарының өнімділігін төмендетумен қатерін төндіреді.

1.3Ақпаратты жоғалту, яғни маңызды ақпаратты кездейсоқ жою.

Электрондық поштаның негізгі ерекшеліктерінің бірі оған формальды қатынаста (коммерциялық коммуникациялардың басқа түрлерімен салыстырғанда) тұрады. Біріншіден, пайдаланушылардың көпшілігі электрондық поштаға уақытша нәрсе ретінде қарайды, яғни "оқыдым және тастадым"принципі бойынша одан түседі. Мұндай жағдайда маңызды ақпаратты кездейсоқ жою қаупі бар. Сонымен қатар, маңызды клиентпен хат жазысуды жоғалту қаупі бар.

1) Ұйымның іскерлік беделіне зиян келтіру.

Электрондық поштаға формальды қатынас, сондай-ақ, электрондық хабарламалардың қысқа мерзімділігіне байланысты адамдар оларды дәстүрлі хаттарда пайдалануға ешқашан мүмкіндік бермейтін өрнектерде сезімдер мен пікір білдіру үшін жиі пайдаланады. Мұндай хаттарды желіде жариялау компанияның беделіне елеулі зиян келтіруі немесе оған қатысты заңды талап-арыздардың себебі болуы мүмкін.

Менің ойымша, электрондық поштаны пайдалану кезінде ақпараттық қауіпсіздіктің жоғарыда сипатталған барлық қатерлеріне назар аудару керек.

Электрондық хат алмасудың барлық ықтимал қатерлерін қамтитын ақпаратты қорғаудың осындай жүйесін құруға тырысу қажет. Менің ойымша, олар кәсіпорын үшін, оның тұрақты жұмысы үшін үлкен қауіп төндіреді. Қорғауға кәсіпорын қызметкерлерінің жұмыс станциялары (пошта клиенттері), сондай-ақ электрондық хат алмасу процесінде жергілікті желі мен интернет желісін пайдаланушылар арасындағы байланыстырушы буын болып табылатын пошта сервері жатады. Жергілікті желіде пошта клиенттері 200-ге жуық жұмыс станциясы болып табылады.

2 Теориялық бөлім

2.1. Электрондық пошта жұмысының негізгі принциптері

1) Электрондық пошта жұмысының ұғымы және жалпы принциптері

Электрондық пошта (e-mail немесе email, SCR. electronic mail) - қызметтің атауы және бөлінген (оның ішінде жаһандық) компьютерлік желі бойынша электрондық хабарламаларды жіберу және алу бойынша ол ұсынатын қызметтер[1].

Массачусет технологиялық институтының (MIT) қызметкерлері Ноэль Моррис пен Том Влек IBM 7090/7094 компьютерінде орнатылған CTSS (Compatible Time-Sharing System) операциялық жүйесіне арналған MAIL бағдарламасын жазған кезде, 1965 жылға Электрондық поштаның пайда болуын жатқызуға болады[2]. Сол уақыттан бастап электрондық пошта жүйелері елеулі өзгерістерге ұшырады. Олардың дамуының бастапқы кезеңдерінде бір жергілікті желі пайдаланушылары бір сервермен қысқа мәтіндік хабарламалармен алмасты. Жаңа функцияларды электрондық поштамен орындау үшін екі адам арасында мәтіндік және екілік ақпаратпен (яғни файлдармен) алмасуға мүмкіндік беретін хаттамалар әзірленді және енгізілді. Осы хаттамалардың көпшілігін дамыту үшін негізгі түрткі Интернет желісінің қарқынды өсуі болды. Бүгінгі күні электрондық пошта адамдардың күнделікті өмірінің ажырамас бөлігі болып табылады, іскерлік қарым-қатынас үшін белсенді қолданылады және Интернет желісінің негізгі сервистерінің бірі болып табылады.

Электрондық поштаның негізгі ерекшелігі-ақпарат алушыға тікелей емес, аралық буын арқылы жіберілгенде-алушы сұрамағанша, хабарлама сақталатын сервердегі орын болып табылатын электрондық пошта жәшігі. Көп жағдайда пошта жәшігіне кіру үшін құпия сөз болуы керек. Пошта серверіне кіру екі жолмен: пошта бағдарламалары және веб-интерфейс арқылы ұсынылуы мүмкін.

Электрондық поштамен жұмыс жасаудың екі нұсқасын да егжей-тегжейлі қарастырайық.

2) Пошталық бағдарлама

Бір немесе бірнеше пайдаланушылардың электрондық пошта хабарларын (бір компьютерде бірнеше есептік жазба болған жағдайда) алуға, жазуға, жіберуге және сақтауға арналған пайдаланушының компьютерінде орнатылған бағдарламалық қамтамасыз ету.

Пошта сервері, электрондық пошта сервері - электрондық пошта жүйесінде хабарламаларды жіберу агенті (ағылш. MTA). Бұл бір компьютерден екіншісіне хабар беретін компьютерлік бағдарлама.

Пошта қызметімен жұмыс істеу үшін SMTP, POP және IMAP хаттамалары қолданылады. SMTP хаттамасы (Simple Mail Transfer Protocol – поштаны таратудың қарапайым ХАТТАМАСЫ) пайдаланушылардан серверлерге және Интернеттің пошта серверлері арасында хабарламаларды

жіберу үшін қолданылады. POP (Post Office Protocol – пошталық хаттама) протоколы пошта қызметі клиенті мен пошта қабылдау сервері арасындағы байланысты қамтамасыз етеді. Бұл функцияны IMAP (Internet Message Access Protocol – Интернет желісінің хабарламаларына қатынау хаттамасы) орындайды, алайда IMAP клиентке серверде сақталатын поштаны басқару бойынша үлкен мүмкіндіктер береді. Пошта серверлері арасында хабарларды беруді қамтамасыз ететін бағдарлама SMTP-сервер деп аталады, ал пайдаланушылардан хабарламаларды қабылдайтын бағдарлама POP - сервер (немесе IMAP-сервер) деп аталады. Өте жиі SMTP сервері және POP сервері бірыңғай сервермен іске асырылады.

Пошта серверлері хаттарды пошта жәшіктерінде сақтайды, олар келіп түскен хаттардың жазбалары бар қарапайым файлдарды білдіреді. Әрбір серверге белгілі бір домен аты беріледі және осы атқа түсетін барлық пошта сервермен көрсетілген мекен-жай (немесе мекен-жай) бойынша жіберілуі тиіс. Пошта қызметінің клиенті пошта клиентінің бағдарламасымен орнатылған Интернетке қосылған кез келген компьютерден серверге хабар жібере алады. Әрбір клиент пошта қызметін теңшеу кезінде (немесе тіркелгіні теңшеу) POP және SMTP серверлерінің домендік атауын, сондай-ақ тіркелгінің кіріс аты мен паролін көрсетуі тиіс.

Алушыға жіберушіден электрондық поштаның 2.1 суреттегі қадамдық өтуінің сипаты (proxy серверді пайдаланбай):

– хат жасау;

– пошта клиентін жөнелтушінің SMTP серверімен қосу;

– SMTP-серверіне пошта кімге және жіберуші кім туралы ақпарат беру;

– SMTP-серверімен адресат пен жіберуші туралы деректердің дұрыстығын тексеру және хатты қабылдау (хат тақырыптары мен денесімен));

– жеткізу кезекке хат қою;

– DNS-адресат доменіне пошта серверлері туралы сұрау (MX-жазбалар);

– жөнелтушінің SMTP серверін ең басымдылығы бар адресаттың пошта серверлерімен біріктіру әрекеті. Егер әрекет сәтсіз болса, адресат доменінің резервтік пошта серверлеріне қосылу әрекеттері жасалады;

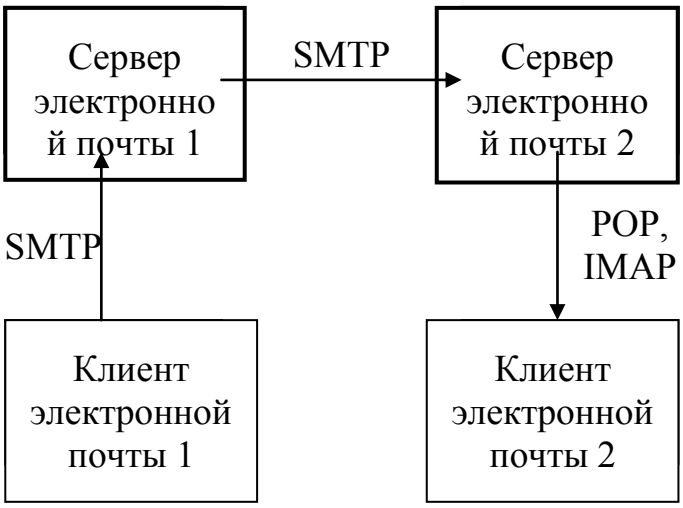
– адресат доменінің пошта серверімен сәтті байланысқан жағдайда хатты жіберу немесе кейін хат жіберу үшін кезекке қою, сәтсіз болған жағдайда;

– хат адресатының SMTP-серверімен қабылдау;

– хатты тексеру оның спам сияқты;

– оны POP3, IMAP хаттамасы бойынша хаттарды сақтаумен және оларды адресаттарға берумен айналысатын модульге немесе басқаларға жіберу;

– адресатты POP3 немесе IMAP серверімен байланыстыру, аутентификация және адресаттың хат алуы.



Сурет 2.1 – Құжат айналымы желісі

3)Ақпарат алмасу

Web-беттер арқылы жүргізіледі. Пошта клиентінің рөлінде Web-браузер, ал пошта сервері рөлінде – серверлік CGI-сценарий болады. Осы пошта арқылы жұмыс істеу әдісі үшін SSL протоколы қолданылуы мүмкін.

Электрондық пошта жұмысының тетігін одан әрі сипаттау үшін келесі ұғымдарды есте сақтау қажет.

Хост (ағылш. Host-қонақтарды қабылдайтын иесі)-қандай да бір интерфейстер бойынша сервер режимінде "клиент-сервер" форматындағы сервистерді ұсынатын және осы интерфейстерде бірегей анықталған кез келген құрылғы. Көбінесе қосымша Түсіндірмесіз" хост " деп TCP/IP протоколының хосты білдіреді. Кез келген басқа хост сияқты, бұл TCP/IP (IP-мекенжай) сервистері ортасында бірегей мекен-жаймен, сондай-ақ қосымша мәтіндік атымен (домендік атау) сипатталады.

Домен-бірегей домен атымен белгіленетін интернет желісінің домендік атауларының иерархиялық кеңістігінің аймағы (тармағы).

Домендік атау - символдық домен аты. Бір домен аясында бірегей болуы керек. Домен толық атауы нүктелермен бөлінген барлық домен атауларынан тұрады. Домендік атау интернет желісінің тораптарын және оларда орналасқан желілік ресурстарды (веб-сайттарды, электрондық пошта серверлерін, желілік сервистерді) адам үшін ыңғайлы нысанда адрестеу үшін қызмет етеді.

DNS (ағылш . Domain Name System-домендік атаулар жүйесі) - IP адресіне хосттың атауын түрлендірудің бөлінген жүйесі. DNS TCP/IP желілерінде жұмыс істейді. Жеке жағдай ретінде, DNS сақтау және өңдеу және кері сұрау, оның IP мекенжайы бойынша хост атауын анықтау.

4) Протокол SMTP

SMTP протоколы электрондық поштаны тасымалдау үшін әртүрлі желілерде жұмыс істеу үшін әзірленген. Алайда, ең толық пайдаланылатын бірі-25 порт арқылы TCP/IP байланысын орнатумен Internet желісі болды. SMTP кең таралуы 1980 жылдардың басында алды. Оған дейін UUCP ХАТТАМАСЫ пайдаланылды, ол жөнелтушіден алушыға дейін толық маршрутты білуді және осы маршрутты алушының мекенжайына анық көрсетуді не жіберуші мен алушының компьютерлері арасында тікелей коммутацияланатын немесе тұрақты қосылыстың болуын талап етті[2]. Қазіргі уақытта SMTP протоколы электрондық пошта үшін стандартты болып табылады және оны барлық клиенттер мен серверлер пайдаланады. Сонымен қатар, әрбір берілген байттың үлкен битін нөлдеуді талап етті. Бұл мәтінді Ұлттық тілдерде (мысалы, кириллица) жіберуге, сондай-ақ екілік файлдарды (суреттер, бейнелер, бағдарламалар немесе мұрағаттар сияқты) жіберуге мүмкіндік бермейді. Бұл шектеуді алып тастау үшін MIME (Multipurpose Internet Mail Extensions - Internet электрондық поштаға арналған көп мақсатты кеңейтулердің форматы) стандарты әзірленді, ол екілік файлдарды мәтіндік файлдарға түрлендіру тәсілін сипаттайды. Қазіргі уақытта көптеген серверлер 8bitmime қолдайды, бұл екілік файлдарды мәтін сияқты оңай жіберуге мүмкіндік береді.

Хабарламаны адресатқа жеткізу үшін оны адресат орналасқан доменнің пошта серверіне жіберу керек. Ол үшін әдетте MX түріндегі жазба қолданылады.

MX немесе Mail Exchanger жазу-белгілі бір доменге арналған пошта жәшіктері үшін жауап беретін серверді көрсететін DNS жазба. Сонымен қатар, MX жазбалары жіберу үшін әрбір ықтимал серверлердің басымдығын көрсетеді.

Белгілі бір мекенжайға электрондық поштаны жіберу үшін сервер-жіберуші DNS-сұрау салады, электрондық хабарламаны алушы доменінің MX-жазбасын (яғни "@"символынан кейінгі мекенжайдың бөліктері) сұратады. Сұрау нәтижесінде осы домен үшін кіріс поштаны қабылдайтын пошта серверлерінің хостарының аттарының тізімі, сондай-ақ әрбір хост үшін басымдық мөлшері қайтарылады. Сервер-жіберуші содан кейін осы хостердің бірімен SMTP байланысын орнатуға тырысады, кем дегенде біреумен байланыс орната алмай тұрып, олардың әрқайсысын таңдап, басымдықтың мәні ең аз адамнан бастап. Егер бірдей басымдылықтары бар бірнеше хосты бар болса, онда олардың әрқайсысымен байланыс орнатуға әрекет жасау керек. MX жазбаларының механизмі бір домен үшін көптеген серверлерді пайдалануға және жүктемені азайту және поштаны сәтті жеткізу мүмкіндігін арттыру мақсатында оларды пайдалануды реттеуге мүмкіндік береді. Сонымен қатар, мұндай механизм кіріс поштаны өңдеуді бірнеше физикалық серверлер арасында таратуға мүмкіндік береді.

Жазба пішімі: хост MX басым мәні.

Мәселен:mail.test.ru үшін пошта ретрансляторы ретінде test.ru 10 басымдығымен келесі жазбаға болады: test.ru ескерту. MX 10 mail.test.ru ескерту.

Егер MX жазба болмаса, онда сол мақсаттар үшін A түріндегі жазба пайдаланылуы мүмкін.

Формат: хост A мағынасы.

Мәселен:test.ru 192.168.0.1 адресіне келесі a-жазба сәйкес келеді: test.ru ескерту.

Сондай-ақ, SRV-жазбасын іске қосуға болады. SRV жазбасы ізделетін қызметтің атын, сондай-ақ осы қызмет жұмыс істейтін протоколды алуға мүмкіндік береді. SRV жазбаларының басымдылығы MX жазбасының басымдығына ұқсас жұмыс істейді: неғұрлым аз басымдық, әсіресе байланысты мақсатты пайдалану жақсырақ. SRV жазбаларының салмағы аймақ әкімшілеріне мақсаттар арасында жүктемені бөлуге мүмкіндік береді. Клиент бір басымдықтың мақсатын олардың салмағына пропорцияда сұрауы тиіс. SRV жазбасы порты іздеу қызметі жұмыс істейтін портты анықтайды.

TURN командасы.

Қауіпсіздік тұрғысынан қызықты SMTP протоколының TURN командасы болып табылады. TCP-қосылысы бойынша екі компьютер арасында екі жақты пошта хабарламаларын алмасуды ұйымдастыру TURN командасын пайдалану МӘНІ БОЛЫП ТАБЫЛАДЫ. Әдетте, SMTP хаттамасымен хабарларды тек бір бағытта бір TCP байланысы арқылы жіберу қарастырылған. Клиенттік хост беру ортасын басқарады және сервердің іс-әрекеттерін SMTP-командалар арқылы жібереді. Пошта клиенттен серверге ғана жіберілуі мүмкін. Бірақ кейде клиенттік машина поштаны серверге жібермей, сервердің клиентке беруі тиіс поштаны қабылдауы қажет. Бұрын талқыланғандай, сеанс ұйымдастырылған Клиентті анықтау үшін сервер HELO командасының көмегімен алынған домендік атауды пайдаланады. TURN командасының мәні серверге клиент рөлдерін өзгертуге және Клиент доменіне бар поштаны жіберуге рұқсат береді. Мұндай алгоритмді қолдану кезінде пайда болатын жалғыз мәселе-клиент қаншалықты сенімді және ол өзі үшін кім болып табылады ма? Егер хакер SMTP серверіне қосылған болса, онда сервер дәл хакердің хостына осы доменге арналған барлық поштаны жіберуге мәжбүр болады.

Бастапқыда SMTP бірыңғай авторландыру схемасын қолдамады. Нәтижесінде спам іс жүзінде шешілмейтін мәселе болды, өйткені іс жүзінде кім жіберуші екенін анықтау мүмкін емес еді. Қазіргі уақытта бұл проблеманы спецификациялардың көмегімен шешуге әрекет жасалуда. Бірыңғай ерекшелік жоқ.

5) Кеңейтілген SMTP хаттамасы (ESMTP)

Алайда уақыт өте келе, SMTP протоколына енгізілген шектеулер байқала бастады. Сол уақытта кең таралған стандартты протоколды ауыстырудың орнына, SMTP протоколының кейбір функцияларын жақсарту

шешілді. Сонымен қатар, SMTP барлық спецификацияларын алғашқы түрде қалдырып, оларға жаңа функцияларды қосу арқылы шешім қабылданды. [3]

Кеңейтілген SMTP (Extended SMTP) келесідей іске асырылды. SMTP сеансының басында HELO командасы шақыру командасына ауыстырылды — EHLO. SMTP серверінің мұндай пәрменді алуы клиент оған кеңейтілген SMTP командаларын жібере алады.

TURN командасының кемшіліктерін өтеу үшін, RFC 1985-да қауіпсіздіктің үлкен деңгейін қамтамасыз ететін жаңа іске асыру анықталған. ETRN командасы SMTP-клиентке хабарламаларды жіберу үшін клиентпен тағы бір SMTP байланысын бастау үшін SMTP-серверге сұраныс беруге мүмкіндік береді. ETRN командасының TURN-дан жалғыз айырмашылығы-сұраныс бар қосылысты пайдалануға емес, жаңа SMTP сеансын ашуға түседі. Осылайша, SMTP сервері клиенттік компьютермен DNS жүйесінің атын түрлендіру алгоритмдерінің әдеттегі көмегімен қосыла алады. Бұл ретте жаңа қосылысты ашу клиенттік компьютер серверде тіркелетін атқа емес, клиенттің хостының нақты атауына негізделеді. Мұндай жағдайда, егер хакер рұқсатсыз SMTP-қосылуды орнатса және ETRN командасын пайдаланса, онда SMTP сервері нақты клиентпен жаңа қосылуды ұйымдастырады және оған электрондық пошта ауысады. Нәтижесінде зардап шеккендер жоқ. Etrn командасының пішімі келесі:

ETRN name

Мұнда name ретінде хосттың аты немесе домен аты болуы мүмкін (егер барлық домен үшін пошта сұралса).

6) Протокол POP

Қазіргі уақытта POP3 протоколын пайдаланады – бұл POP протоколының үшінші нұсқасы, алдыңғы нұсқалары (POP, POP2) ескірген. POP3 протоколының стандарты RFC 1939-да анықталған.

POP3 протоколы арқылы жұмыс істеу алдында сервер 110 портын тыңдайды. Клиент осы протоколды пайдаланғысы келген кезде, ол сервермен TCP байланысын жасау керек. Байланыс орнатылған кезде, сервер шақыру жібереді. Содан кейін клиент пен POP3 сервер байланыс жабылмаған немесе үзілгенше ақпарат алмасады.

POP3 пәрмендері негізгі сөздерден тұрады, кейбіреулер бір немесе одан да көп аргументтер керек. Барлық командалар CRLF жұпымен аяқталады (жолды аудару белгісі). Кілт сөздер мен аргументтер басылатын ASCII таңбалардан тұрады. Кілт сөз мен аргументтер бір бос орынмен бөлінген. Негізгі сөз 3-тен 4 символға дейін, ал дәлел 40 символға дейін болуы мүмкін.

POP3-дегі жауаптар күй индикаторынан және қосымша ақпарат алуы мүмкін кілт сөзінен тұрады. Жауап CRLF жұбымен аяқталады. Тек екі күй индикаторы бар: "+OK" - оң және "-ERR" - теріс. Кейбір командаларға жауаптар бірнеше жолдан тұруы мүмкін. Бұл жағдайда әрбір жол CRLF жұпымен бөлінген, ал жауаптың соңы ASCII 46 символымен аяқталады (".") және бу CRLF.

POP3 хаттамасында сеанстың 3 күйі қарастырылған:

– авторизация-клиент аутентификация рәсімінен өтеді. Бұл жағдай сервермен байланыс орнатылғаннан кейін басталады және сервер шақыру жібереді.

– транзакция-клиент пошта жәшігінің жағдайы туралы ақпаратты алады, серверді белгілі бір пәрмендерді орындауға сұратады;

– жаңарту-сервер таңдалған хаттарды жояды, барлық жұмыс істейтін ресурстарды босатып, қосылымды жабады. Клиент QUIT командасын жібергенде пайда болады.

POP3 клиенті сервермен TCP байланысын орнатқаннан кейін, ол өзін анықтау керек. Бұл бір мезгілде хабарлар олар арналған пайдаланушыға жіберілгенін растау болып табылады. POP3-дегі пайдаланушының түпнұсқалығын стандартты тексеру пайдаланушы идентификациясы мен user/PASS паролі үшін пәрмендер жиынтығы арқылы жүзеге асырылады. Серверде тіркелген кезде пайдаланушының идентификаторы мен паролін беру мәтіндік түрде жүзеге асырылады. Бұл әдіс қауіпті, сондықтан қосудың тағы екі жолы жасалды: AUTH командасы және APOP командасы арқылы.

USER/PASS командалары.

USER/PASS командаларының комбинациясы — іске асыру үшін ең оңай, бірақ қауіпсіздік тұрғысынан ең қауіпті. Клиент POP3 серверімен байланысқан сайын желі арқылы поштаны тексеру мақсатында оның пайдаланушы идентификаторы және ASCII пішіміндегі мәтін түріндегі пароль жіберіледі.

Бұл командалардың пішімі келесі:

– USER username.

– PASS password.

Username рөлінде POP3 серверіне арналған пайдаланушы идентификаторы болады. Тиісінше, password параметрі осы пайдаланушы идентификаторы үшін құпия сөзді білдіреді. POP3 серверінің жалғыз қорғауы сервердің пайдаланушы идентификаторының дұрыс еместігі туралы клиентке жауап қайтармауы және құпия сөзді енгізуді күтуі болып табылады. Бұл хакерлердің осы POP3 хост үшін пайдаланушының дұрыс идентификаторларын таңдау мүмкіндігін болдырмайды.

AUTH командасы.

Пайдаланушыны тіркеу кезінде қауіпсіздікті арттырудың тағы бір әдісі-RFC 1734-де сипатталған AUTH командасын қолдану. Команда IMAP протоколынан алынды.

AUTH командасының пішімі келесі: AUTHmechanism

Mechanism параметрі Клиентті серверге қосатын пайдаланушының шынайылығын тексеру әдісін анықтайды. Пайдаланушыны тексеру әдісі келісілген кезде пайдаланушының идентификаторының түпнұсқалығын тексеру күшіне енеді. Клиент шынайылықты тексеру әдісі келісілетін сервермен келіссөздер сеансын бастамашылық етеді. Алдымен клиент ең жоғары ықтимал шифрлау дәрежесі бар AUTH командасын береді. Егер сервер тиісті шифрлау деңгейін қолдамаса, ол теріс жауапты қайтарады.

Содан кейін клиент тағы бір AUTH командасын бере алады. Клиент пен сервер арасындағы бұл келіссөздер клиент пен сервер екі түпнұсқа тексеру алгоритмі үшін қолайлы тапқанға дейін жалғасады, әйтпесе олар жай ғана USER/PASS командалардың комбинациясын пайдалануға көшеді.

APOP командасы.

POP3 серверіне кіру үшін, USER / PASS командалардыңкомбинациясының орнына, клиент APOP командасын пайдалана алады. APOP командасы клиентке мәтіндік түрде құпия сөзді жібермей серверде тіркеуге мүмкіндік береді, — ол MD5 алгоритмі арқылы шифрланған құпия сөзді қолданады. APP командасының пішімі: APP name digest

Name аргументі-серверде тіркелетін пайдаланушының әдеттегі идентификаторы. Digest параметрі клиентке MD5 кодталған digest мәнін жіберу мүмкіндігін береді,оның көмегімен пайдаланушының түпнұсқалығын тексеру жүргізіледі. MD5 шифрлау алгоритмін Рон Райвест (Ron Rivest) жасап, RFC 1321 құжатында сипатталған. Бұл алгоритм құпия сөзге (кілтке) белгілі хабарлама қою үшін хеширлеу алгоритмін қолдануға негізделген, ол тек екі шеткі нүктеге белгілі. Хеширлеу алгоритмінің белгісі-клиенттің атымен бірге берілетін digest параметрінің болуы. Мұндай схеманың қалыпты жұмыс істеуі үшін клиент пен серверге кілт алдын ала белгілі болуы керек. Кілтке орнатылған белгілі хабар ретінде, оған TCP байланысы орнатылған кезде POP3 серверін шақыру болуы мүмкін. Әдетте, мұндай хабардың рөлінде POP3 серверінің хост аты болатын идентификатор болады.

Дегенмен, APOP командасының қолдауы POP3 протоколы үшін міндетті емес екенін атап өту керек. POP3 серверінің шақыруын талдай отырып, бұл команда сервермен қолдау көрсететінін тексеріңіз.

TLS және SSL қолдайтын POP3 серверлерін іске асыру бар.

Пошта серверінен хабарларды жинау үшін балама хаттама IMAP болып табылады.

7) IMAP протоколы

Interactive Mail Access Protocol-электрондық поштаға интерактивті қатынау хаттамасы.

IMAP протоколы клиентке пошта серверінде әр түрлі қалталар жасап, онда сақтау үшін Хабарлар қоюға мүмкіндік береді. IMAP хаттамасы бойынша пошта серверімен байланыс кез келген жұмыс станциясынан орнатылуы мүмкін. Бұл ретте пайдаланушылар сол папкалар мен пошта жәшіктеріне қол жеткізеді. Ең бастысы-хабарлар тек көрсету үшін жұмыс станциясына жүктеледі. Олардың көшірмелері клиентке жүктегенге дейін сақталған папкада серверде қалады. Электрондық хаттармен болады айла-шарғы емес, компьютер пайдаланушы (клиент) қажеттілігісіз тұрақты жіберу серверден және кері файлдарды толық хаттың мазмұны. Хаттарды жіберу үшін SMTP хаттамасы қолданылады.

IMAP қарапайым POP3 протоколын ауыстыру үшін әзірленген және соңғы салыстырғанда келесі артықшылықтары бар:

– хаттар клиентте емес, серверде сақталады

– әртүрлі клиенттерден бір пошта жәшігіне кіруге болады. Сондай-ақ, бірнеше клиенттердің бір уақытта қатынауына қолдау көрсетіледі. Хаттамада клиент басқа клиенттер жасаған өзгерістер туралы хабардар болуы мүмкін механизмдер бар;

– бірнеше пошта жәшіктерін (немесе қалталарды) қолдау. Клиент сервердегі пошта жәшіктерін жасап, алып тастай алады және бір пошта жәшігінен екінші пошта жәшігіне ауыстыра алады;

– бірнеше пайдаланушылар қол жеткізе алатын ортақ қалталарды жасауға болады;

– хаттардың күйі туралы ақпарат серверде сақталады және барлық клиенттерге қол жетімді. Хаттар оқылған, маңызды және т. б. ретінде белгіленуі мүмкін;

– серверде іздеуді қолдау. Бір орынды табу үшін серверден көптеген хабарламаларды жүктеудің қажеті жоқ;

– онлайн-жұмысты қолдау. Клиент сервермен тұрақты байланыс жасай алады, бұл ретте сервер нақты уақытта Клиентті пошта жәшіктеріндегі өзгерістер туралы, оның ішінде жаңа хаттар туралы хабардар етеді;

– хаттама мүмкіндіктерін кеңейту тетігі қарастырылған.

Хаттаманың ағымдағы нұсқасы IMAP4rev1 (IMAP, 4 нұсқасы, ревизия) белгісі бар. IMAP 4.1 байланысы клиент пен сервер арасында байланыс орнатуды білдіреді. Клиент серверге команданы, серверді клиентке сұрау салуды орындау мәртебесі туралы деректерді және хабарламаларды жібереді. Клиент пен сервердің барлық хабарламалары CRLF ретімен аяқталатын жол пішінінде болады. Алушы (клиент немесе сервер) осы жолды немесе жол өтетін белгілі ұзындықтағы октеттердің бірізділігін қабылдайды.

Хаттама шифрланған түрде пайдаланушының құпия сөзін жіберуді қолдайды. Сонымен қатар, IMAP-трафикті SSL көмегімен шифрлауға болады[4].

8) SSL хаттамасы

SSL (Secure Sockets Layer-қорғалған сокеттер ХАТТАМАСЫ)-бұл web-сервер мен пайдаланушының браузері арасындағы байланыс арнасының қауіпсіздігін қамтамасыз ететін хаттама. Оны пайдалану кезінде құрылады қорғалған байланыс клиент пен сервер арасында. SSL бастапқыда Netscape Communications компаниясы әзірлеген. Нәтижесінде SSL 3.0 хаттамасы негізінде TLS атын алған RFC стандарты әзірленді және қабылданды.

SSL протоколының екі деңгейі бар: жазбалар ХАТТАМАСЫ (SSL Record Protocol) және диалог ХАТТАМАСЫ (SSL Handshake Protocol). Соңғысы клиент пен серверге бір-бірін сәйкестендіруге, белгілі бір шифрлау алгоритмін пайдалануды келісуге және кілттермен алмасуға мүмкіндік береді.

SSL хаттамасы келесі функцияларды іске асырады[5]:

– қосылымның құпиялылығы алдын ала диалогтан кейін симметриялық криптография үшін пайдаланылатын құпия кілт анықталады (мысалы, des немесе rc4);

– серіктестер бір-бірін асимметриялық криптографиялық әдістердің (мысалы, RSA немесе DSS);

– қосылудың сенімділігін қамтамасыз ету. Жіберу Mac (Message Autentification Code) аутентификация кодын және функциялардың хэшін (SHA немесе MD5) қолдана отырып хабарлардың бүтіндігін бақылауды қамтиды.

Таратқыштың және алушының түпнұсқалығын растау ашық кілтпен шифрлауға негізделеді. Деректер берудің сенімділігі түзетуші кодтар мен қауіпсіз хэш-функцияларды пайдалану есебінен жүзеге асырылады.

SSL протоколы клиент пен сервердің бір күйден екіншісіне ауысуын көздейді. Әрбір рәсім объектінің қатаң белгіленген жағдайында іске асырылады. SSL протоколының диалогтық бөлігі клиент пен сервердің күй машиналарының жұмысын үйлестіруге мүмкіндік береді. Логикалық кез келген күй екі рет, жұмыс (operating) күйі және қарастырылған күйі (pending) ретінде ұсынылады. Сонымен қатар, оқу және жазу жағдайлары да қарастырылған. Клиент немесе сервер "change cipher spec" хабарын алған кезде, ол қаралып отырған жағдайды ағымдағы оқу күйіне көшіреді. "Change cipher spec" хабарын жібергенде, клиент немесе сервер ағымдағы жазба күйіне осы күйдегі жағдайды көшіреді. Келісу диалогы аяқталған кезде клиент пен сервер "change cipher spec" хабарламаларымен алмасады, содан кейін келісілген шифрлау ерекшелігін пайдалана отырып, бір-бірімен өзара әрекеттеседі. SSL хаттамасы Бір сессия шеңберінде клиент пен сервер арасындағы қосылыстардың кез келген санына жол береді.

2.2 Электрондық хат алмасу және электрондық пошта сервистеріне қауіп-қатерден қорғау әдістерін шолу

1)Құпиялылық қатері.

Пошта хабарламаларының құпиялылығын ашудан қорғау үшін шифрлауды пайдалану қажет. Жоғары өнімділік пен тұрақтылық арқасында симметриялы шифрлау пошта жіберулерін шифрлау үшін пайдаланылуы мүмкін. Алайда, кілттерді тарату проблемасы бар. Қажетті қорғаныс деңгейін қамтамасыз ету үшін кілтті әдетте шифрланған ақпаратты тарату арнасынан ерекшеленетін арналар арқылы береді. Бұл ретте пайдаланушыны сенімді сәйкестендіру (оның шифрланған ақпаратқа рұқсат етілген рұқсаты болуы тиіс) және құпиялылық (беру процесінде кілтке қол жеткізуді болдырмау) қамтамасыз етілуі тиіс.

Тағы бір мәселе-парольдерді ұстау. Егер қаскүнем пайдаланушының атын және POP-сервердің (немесе IMAP-сервердің) есептік жазбасының паролін ұстай алса, жоғарыда айтылған шаралар кез келген өзектілігін жоғалтады. Осы қауіп түрінен қорғаудың ең қарапайым әдісі-пошта клиенттерін пайдаланудан бас тарту және пошта қызметтерінің Web-интерфейсін пайдалануға көшу. Құпия деректерді жіберу кезінде SSL

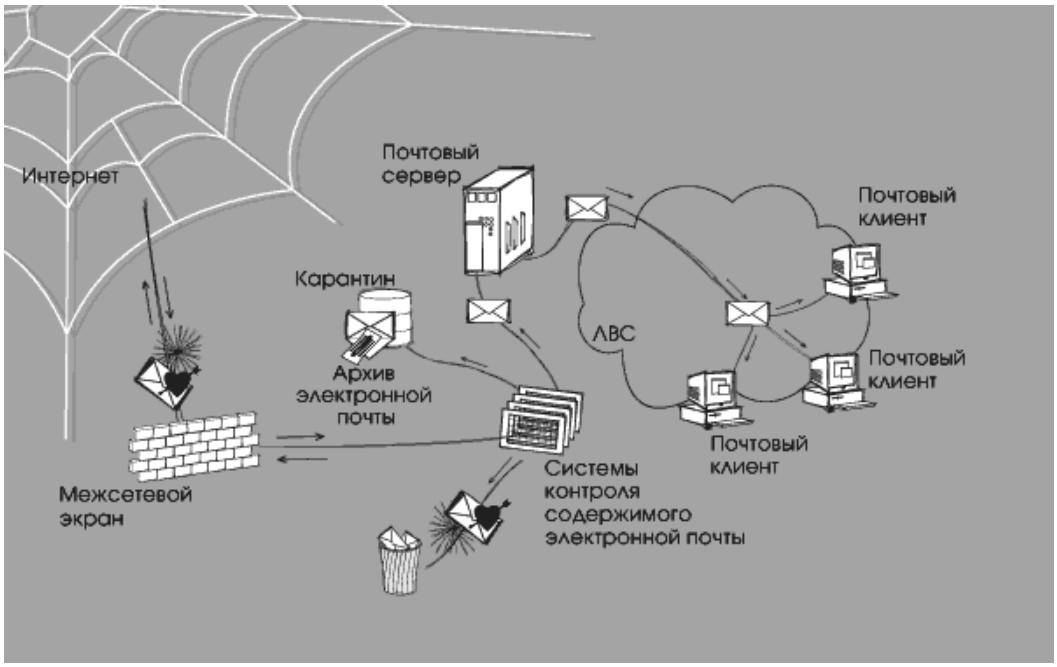
қолдайтын қорғалған режимді пайдаланатын пошта сервистеріне басымдық беру керек. Бұл шешім үй желілерінің жағдайы мен ақпараттық қауіпсіздік тұрғысынан пошта клиенттерінің жұмысын дербес реттей алмайтын пайдаланушылар үшін ең қолайлы. Тәжірибелі пайдаланушылар үшін қауіпсіз авторландыруды қолдау үшін пошта клиенттерінің жұмысын теңшеу нұсқасы мүмкін.

Осы ақпаратты ұйым қызметкерлерінің таратуы тұрғысынан құпия ақпараттың жария болуы құпиялылық қатерлерінің бір бөлігі болса да ерекше қорғау әдісі – контент-талдау әдісін қолдануды талап етуге байланысты бөлінуі мүмкін.

Контент-талдау (ағылш. contents-мазмұны, мазмұны) – мәтін массивтерінің және коммуникативтік хат-хабар өнімдерінің мазмұнын талдау пәні бар қоғамдық ғылымдар саласындағы зерттеудің стандартты әдістемесі. Бізді қызықтыратын пәндік салада контент-талдау түрлі компоненттер мен құрылым бойынша электрондық хат мазмұнына қолданылады. Мұндай талдау үшін арнайы электрондық пошта мазмұнын бақылау жүйелері қолданылады. Жүйе кіріс және шығыс пошта трафигін талдау үшін саясаттар, ережелер, сүзгілер жиынтығы болып табылады[6].

Пошта желідегі 2.2 суреттегі сипатталған ағында екі серверден тұрады:

– пошта ағынын талдау;
– пошта хабарламаларын сақтау.



Сурет 2.2 – Поштаның желідегі ағын түрі

"Үзілу" режимі, online тексеру жүргізілген кезде, жүйенің жоғары сенімділігі, тұрақты жұмыс, жоғары жылдамдық және тиісінше оған қызмет көрсету сапасы болуы тиіс. Мұнда жоғары жылдамдық мазмұнды online талдау үшін қажет-барлық хаттарды соңғы құрауыштарға дейін бөлшектеу,

саясатқа сәйкестігін тексеру, ереже бұзылған жағдайда әрекет ету және осы және басқа да электрондық хат-хабарларды ұзақ уақыт бойы кідіртпеу.

"Тармақталу" режимі біз хаттарды сақтау қоймасына жоғары талаптар мен оның жұмыс жылдамдығына қойылатын басқа кластағы жүйеге ие болдық, өйткені ол негізгі жұмыс болып табылады – берілген шарттар бойынша хаттарды іздеу. Мысалы, хат тақырыбы бойынша "есеп"сөзімен белгілі бір доменнен хат алу күні бойынша. Міне, жүйенің қарапайым үлгісі

– антиспам (тек кіріс пошта);

– антивирус (кіріс және шығыс);

Әрі қарай контент-тексеру жүргізіледі:

– топ менеджменттің хаттары (акционерлер және компания басшылары) тексеруден өтпейді және хаттардың жалпы базасына енгізілмейді;

– бөлімше бастықтарының хаттары барлық сүзгілерден өтеді және тиісті белгілермен және/немесе әкімшіге хабарламалармен базаға жинақталады (инцидентті және/немесе бұзушылықтарды кейіннен тексеру мүмкіндігі үшін);

– қалған қызметкерлердің хаттары барлық сүзгілерден өтеді және белгілі бір жағдайларда кідіртіледі, жүйе әкімшісі бұзушылықтарды одан әрі тексеру үшін хаттың көшірмесімен хабарлама алады.

Сүзгілер туралы толығырақ айтамыз:

– жіберушінің белгілі бір пайдаланушы топтарына жататын сүзгілер (біздің мысалда бұл TOP менеджерлер, бастықтар, қатардағы қызметкерлер);

– қорғау және/немесе криптография қолданылатын хаттар, парольмен жабылған мұрағаттар мен файлдар;

– алушыға арналған сүзгілер: хат-хабарларды өкілдікке және достас компанияларға "құпия" және "криптографияны пайдалану" белгілері бар хаттарды жіберуге рұқсат»;

– құпия сөздер мен сөз тіркестерінің мазмұнына сүзгілер;

– жұмыс іздеу сүзгілері (Түйіндемені жіберу);

– бәсекелестермен қарым-қатынас сүзгілері;

– өзге де арнайы сүзгілер (компания бизнесіне жауап беретін).

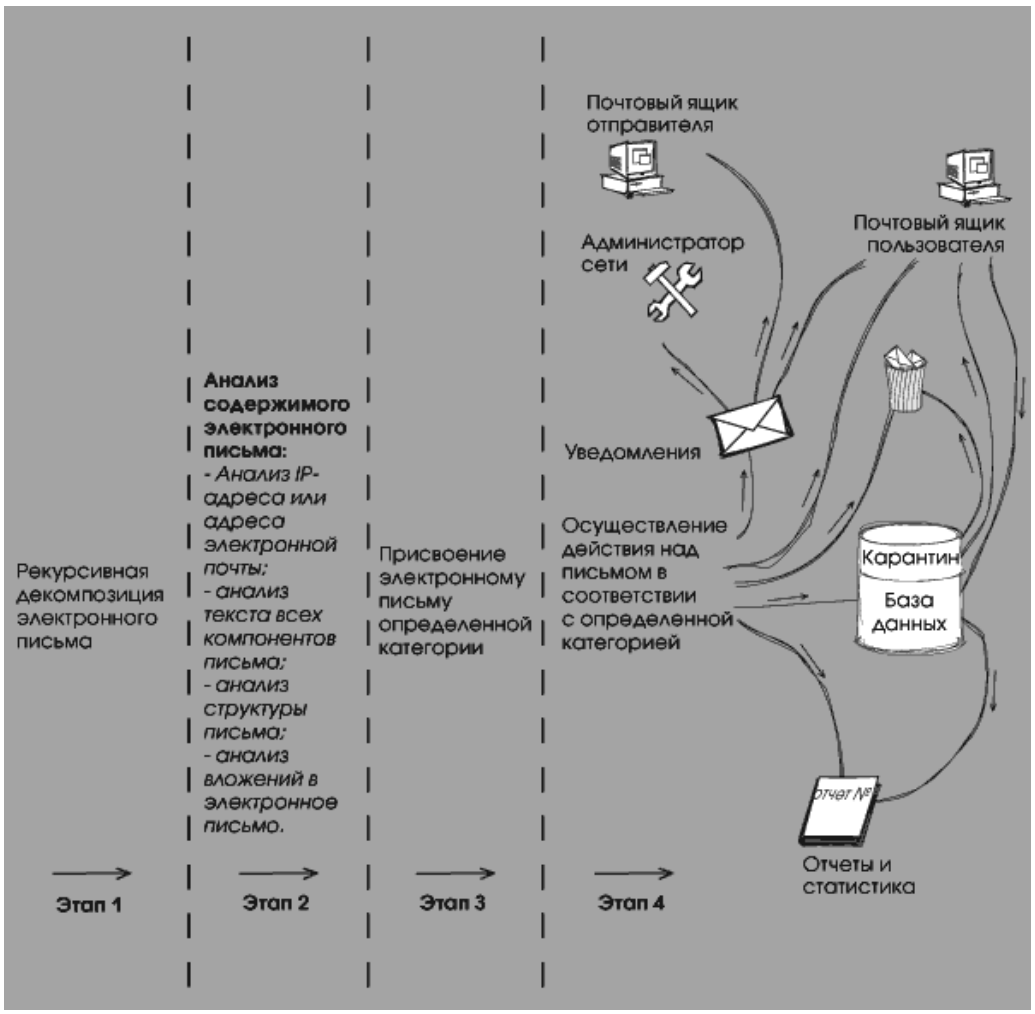
2.3 суреттегі сипатталған шлюз реакциялары:

– хатты ұстау және жауапты тұлғаларды бұзушылық туралы хабарлау;

– бұзушылық туралы жауапты тұлғаларға хабарлама және хат жіберу;

– қалаусыз хат элементін кесу және жауапты тұлғаларды бұзушылық туралы ескерту;

– спецификалық сүзгілер (компания бизнесіне жауап беретін).



Сурет 2.3 – Пошта шлюздан өтер кезеңдері

Компанияның үлкен пошта ағындары кезінде, біз контент - талдау серверіне үлкен жүктememен айналысамыз. Көрсетілген қарапайым ережелермен, сүзгілермен және жүйенің реакцияларымен біз әдеттегі пошта серверлеріне жүктемесінен 6 есе артық жүктемеге ие болдық.

2)Аутентификация қаупі.

Қауіп-қатердің осы түрімен күресу үшін ашық кілттер сертификаттары негізінде ЭЦҚ тетігін пайдалану қажет. Дәлме-дәлдік проблемасы жеке тұлғаға қарағанда кәсіпорындар үшін көп дәрежеде өзекті, сондықтан ЭЦҚ-ның жұмыс істеуіне белгілі бір шығындардың болуын оны пайдалану үшін тежеуші фактор деп санауға болмайды.

3)Хабарламалардың тұтастық қатері.

Бұл қауіптер түрінен қорғау әдістері HMAC және электрондық цифрлық қолтаңбаны пайдалану болып табылады[7].

4) Бас тарту немесе терістеу қатері.

Қауіптердің бұл түрі ЭЦҚ пайдалану есебінен бейтараптандырылады.

5) Зиянды бағдарламаларды енгізу.

Бұл қатерден құтылуға тек "қауіпті" тіркемесі бар хаттарды бұғаттау, сондай-ақ тіркелген файлдарды вирусқа қарсы тексеру арқылы ғана болады.

Практикада белгілі бір файл түрлерін құлыптау оңтайлы құрал болуы мүмкін. Бұл әдетте орындалатын файлдар (exe, com, bat) және макростар мен OLE нысандары (MSOffice бағдарламаларында жасалған файлдар) бар файлдар.

6) Спам

1) Бірінші әдістеме спамды анықтау әдісін іске асыратын антиспам сүзгілерінде қолданылады, хатта негізгі сөздер немесе сөз тіркестерінің бар болуы, хат тақырыбын сипаттап жазу (Мысалы, барлық бас әріптер және леп белгісі көп), сондай-ақ ерекше мекенжай ақпараты.

2) Екінші әдіс жіберушінің мекен-жайын және оның OpenRelayBlackList (ORBL) пошталық серверлерінің "қара тізімдеріне" жататынын анықтаумен байланысты.

3) Бұл тізімдерге спамның жаппай таратуларында байқалған немесе нақты пайдаланушы немесе қара тізімді ұстаушы ұйым қалыптастырған критерийлерге сай келмейтін серверлер енгізіледі. Идея осы серверлерден шығатын поштаны мүлдем қабылдамауға және таратпауға тұрады.

4) Үшінші әдістеме екі тізбеден тұрады, бірақ өнімділігі жағынан бірінші екіден айырмашылығы аз.

Екі әдісті қолдану арқылы жақсы бапталған сүзгіні тестілеу нәтижелері 100% спам-хабарламалардың тек 79,7% - ы анықталатынын көрсетеді. Бұл ретте жалған іске қосылудың айтарлықтай пайызы анықталды, бұл спамаға қарапайым хаттар жатқызылды (ұсталған хаттардың 1,2%). Бұл жағдайда пайдаланушылар үшін маңызды ақпаратты жоғалту қаупі бар. Спам мен қарапайым хаттардың сапасыз бөлінуі стандартты сүзгілердің кейбір "бірбақылығымен"байланысты. Хаттарды жарамсыз ету кезінде "жаман" белгілері ескеріледі және пайдалы хат алмасуға тән "жақсы" белгілері ескерілмейді.

1) Бұл кемшіліктерден американдық бағдарламашы мен кәсіпкер Пол Грэм ұсынған төртінші әдістеме жоғалды. Ол жеке хат алмасу ерекшеліктеріне сәйкес сүзгілерді автоматты түрде баптауға мүмкіндік береді,ал өңдеу кезінде "нашар" және "жақсы" сүзгілердің белгілерін ескереді.

2) Әдістеме Ықтималдықтар теориясына негізделеді және спамды сүзу үшін Байес статистикалық алгоритмін қолданады. Қолда бар бағалаулар бойынша, бұл спаммен күрес әдісі өте тиімді. Мәселен, сынақ барысында сүзгі арқылы 8000 хат жіберілді,оның жартысы спам болып табылады. Нәтижесінде жүйе тек 0,5% спам-хабарламаларды тани алмады, ал сүзгінің қате іске қосылу саны нөлдік болды.

3) Спаммен күресу әдістері контент-талдау жүйелеріне, сондай-ақ құпия ақпараттың таралып кетуінен қорғау әдістеріне негізделеді. Сондықтан контент-талдау жүйелеріне электрондық пошта қатерлерінен қорғау жүйелерін құру кезінде айтарлықтай үлкен көңіл бөлінеді.

4) Ақпаратты жоғалту, яғни маңызды ақпаратты кездейсоқ жою.

5) Мәселелер ұйымда электрондық пошта мұрағатын құру арқылы шешіледі.

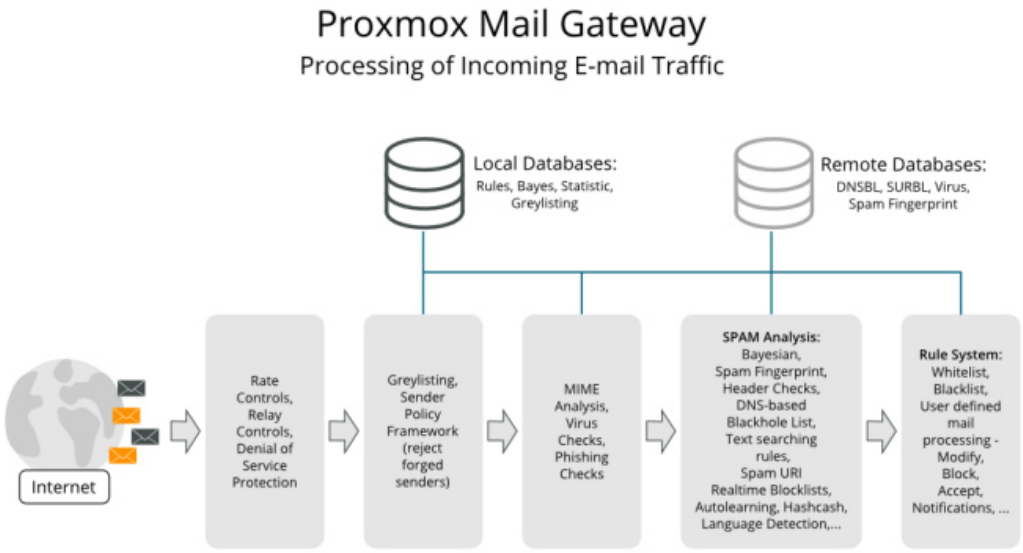
6) Ұйымның іскерлік беделіне зиян келтіру.

7) Бұл мәселе ұйымда электрондық поштаны пайдалану саясатын әзірлеу және қолдану, сондай-ақ контент-талдау әдістерімен шешілуі мүмкін. Сұрақ поштаны пайдалану саясаты біз келесі тараулардың бірінде қарастырамыз.

3 Техникалық бөлім

3.1 Proxmox пошта шлюзі дегеніміз не?

Электрондық пошта қауіпсіздігі барлық кіріс және шығыс электрондық пошта хабарларын бақылау арқылы шлюзден басталады. Proxmox пошта шлюзі 3.1 суреттегідей сипатталған спам және вирустарды табу арқылы қалаусыз пошта трафигін толық спектрін жібереді. Proxmox Mail Gateway сіздің пошта жүйесінен спамды, вирустарды жою және қалаусыз мазмұнды құлыптау үшін қуатты және қолжетімді серверлік шешім ұсынады. Барлық өнімдер өздігінен тоқтайды және Linux терең білімсіз пайдаланылуы мүмкін.



Сурет 3.1– Пошта трафигінің өтетін жолы.

3.2 Ерекшеліктері

1) Спамды анықтау

Proxmox пошта шлюзі спам-поштаны анықтау үшін жергілікті және желілік тесттердің кең спектрін пайдаланады. Мұнда қолданылатын сүзу әдістерінің қысқаша тізімі.

2) Қабылдағышты Тексеру

Сіздің желіңізге жететін қалаусыз хабарламалардың көпшілігі - жоқ пайдаланушыларға электрондық хаттар. Proxmox пошта шлюзі SMTP деңгейінде осы хаттарды анықтайды, яғни оларды желіде жібергенге дейін. Бұл спам мен вирустарға талдау жасау үшін трафикті 90% - ға дейін азайтады және пошта серверлері мен сканерлерге жұмыс жүктемесін төмендетеді.

3) Sender Policy Framework (SPF)

Sender Policy Framework (SPF) - бұл электрондық поштаны тексеру және жіберушінің IP-адресін қолдан жасауды болдырмаудың ашық стандарты. SPF интернет доменінің әкімшісіне домендік атаулар жүйесінде (DNS) SPF

белгілі бір жазбасын жасап, осы доменмен электронды хаттарды жіберуге қандай компьютерлерді көрсетуге мүмкіндік береді.

4) DNS негізінде блэкхол тізімі

DNS (DNSBL) негізіндегі қара дыр тізімі - бұл интернет-сайт интернеттегі компьютерлік бағдарламалармен оңай сұралуы мүмкін пішімдегі IP-адрестер тізімін жариялай алатын құрал. Технология домендік атаулар жүйесінің үстіне салынған. DNSBLs спаммен байланысты мекенжайлар тізімін жариялау үшін қолданылады

5)SMTP ақ тізімі

SMTP блоктан жіберушілерді алып тастау. Барлық SMTP тексереді (сұр, SPF тексеру қабылдағышы және РБЛ) және жүйе ережелерін сүзгіде талдау үшін барлық поштаны қабылдай аласыз, сіз осы тізімге: домендер (жіберушінің/алушының), пошта мекен-жайы (жіберушінің/алушының), тұрақты өрнек (жіберуші/алушы), IP-мекен-жайы (жіберушінің), IP-желісі (жіберушінің / алушының) қосуға болады.)

6)Байесовский сүзгісі-автоматты түрде оқитын статистикалық фильтр

Кейбір нақты сөздер заңды хаттарда емес, спам-хаттарда пайда болу ықтималдығы жоғары. Байесовский әр электрондық поштаны тексереді және бұл спам сөз немесе оның базасында жоқ деген ықтималдығын түзетеді. Бұл автоматты түрде жасалады

7)Қара-ақ тізімдер

Қара және ақ тізімдер-алушыларға хаттарды қабылдау, бұғаттау немесе карантин үшін қол жеткізуді бақылау тетігі. Бұл домендер, электрондық пошта мекен-жайы, тұрақты өрнек, IP желісі, LDAP тобы және т.б. сияқты түрлі нысандарды қолдану арқылы ереже жүйесін реттеуге мүмкіндік береді.

8)Автоматты оқыту алгоритмі

Proxmox пошта шлюзі спам хаттары туралы статистикалық ақпаратты жинайды. Бұл ақпарат автоматты оқыту алгоритмімен пайдаланылады, сондықтан уақыт өте келе жүйе Ақылды болады.

9)Нақты уақытта spam Uri құлыптау тізімі (SURBL)

SURBLs хабар денесінің URI негізінде спамды анықтау үшін қолданылады(әдетте веб-сайттар). Бұл SURBLs спам жіберушілерді бұғаттау үшін пайдаланылмайды, өйткені нақты уақытта басқа блоктау тізімдерінің көпшілігінен оларды ажыратады.SURBLs хабарлар денелерінде айтылған спам-хост хабарларды бұғаттауға мүмкіндік береді.

10)Қолдау листі

Greylisting жіберушіден хат сіздің жүйе танымайды, ол уақытша қабылданбайды дегенді білдіреді. Уақытша іркілістер поштаны жеткізу үшін RFC ерекшелігіне енгізілген болғандықтан, заңды сервер электрондық хатты кейінірек қайта жіберуге тырысады. Бұл тиімді әдіс, себебі спамерлер кезекте тұрмайды және әдетте әдеттегі пошта көлігі агенті үшін поштаны жеткізуге тырыспайды. Greylisting электрондық пошта трафигін 50% дейін азайтуы мүмкін. Сұр хат Сіздің пошта серверіне ешқашан жетеді, және осылайша, сіздің пошта сервері пайдасыз "жеткізбеу есептер" спамерлерді жібермейді.

1)Вирустарды табу

Proxmox пошталық шлюзі трояндарды, вирустарды, зиянды бағдарламаларды және басқа да зиянды қауіп-қатерлерді анықтауға арналған Ашық бастапқы коды (GPL) бар антивирустық ядро болып табылатын ClamAV® біріктіреді. Ол mutli-threaded Scanning daemon жоғары өнімділігін қамтамасыз етеді, талап бойынша файлдарды сканерлеу үшін командалық жолдың утилиттері және қолтаңбаны автоматты түрде жаңарту үшін зияткерлік құралы.

2) Ережелердің Объектілі-Бағытталған Жүйесі

Объектілі-бағытталған ереже жүйесі домендерге арналған теңшелетін ережелерді қамтиды. Бұл қарапайым, бірақ өте қуатты әдіс пайдаланушы, Домен, уақытша рамалар, контент түрі және нәтиже нәтижесі бойынша сүзу ережелерін анықтау. Proxmox Пошталық Шлюзі өз пайдаланушы жүйесін реттеу үшін көптеген қуатты нысандарды ұсынады.

Әрбір ереже бар бес санат FROM, TO, WHEN, WHAT және ACTION. Осы санаттардың әрқайсысы бірнеше нысан және бағыт (in, out немесе екеуі де) [8].

Параметрлер спам-және вирусты сүзгілердің қарапайым параметрлерінен Электрондық поштаның белгілі бір түрлерін блоктайтын және хабарлама жасайтын күрделі, жоғары теңшелетін конфигурацияларға дейін өзгереді.

3) Спам карантин

Сәйкестендірілген спам-хаттар карантин пайдаланушыға қолжетімді болуы мүмкін. Осылайша, пайдаланушылар өз спам-хабарламаларын өз бетінше көре және басқара алады.

4) Бақылау және жүргізу журналы

Proxmox инновациялық хабар қадағалау орталығы барлық қол жетімді журналдарды бақылайды және жинақтайды. Веб-интерфейс және пайдаланушы үшін ыңғайлы ат басқару интерфейсі арқасында бір экраннан барлық мүмкіндіктерді оңай қарап, басқара алады.

Хабарламаларды қадағалау орталығы өте жылдам және қуатты, күніне миллионнан астам хаттарды өңдейтін Proxmox пошта шлюздерінің сайттарында сыналған. Журналдың барлық әр түрлі файлдары соңғы 7 күн ішінде сұралуы мүмкін және нәтижелері интеллектуалды алгоритммен жинақталады.

- әлектрондық поштаның келуі;
- нәтижелері бар Proxmox сүзуді өңдеу;
- ішкі кезек сіздің пошта серверіне;
- мәртебесі соңғы жеткізу.

5) Интеграцияны өңдеу

Proxmox пошта шлюзі басқа IMAP немесе POP3 серверлерінен поштаны алуға мүмкіндік береді.

6) Пайдаланушыларды икемді басқару

Басқару интерфейсі келесі рөлдерді пайдалана отырып, рөлдер негізінде қатынауды басқару схемасын пайдаланады:

Superuser – бұл рөл барлық жасауға мүмкіндік береді (root пайдаланушысы үшін сақталған).

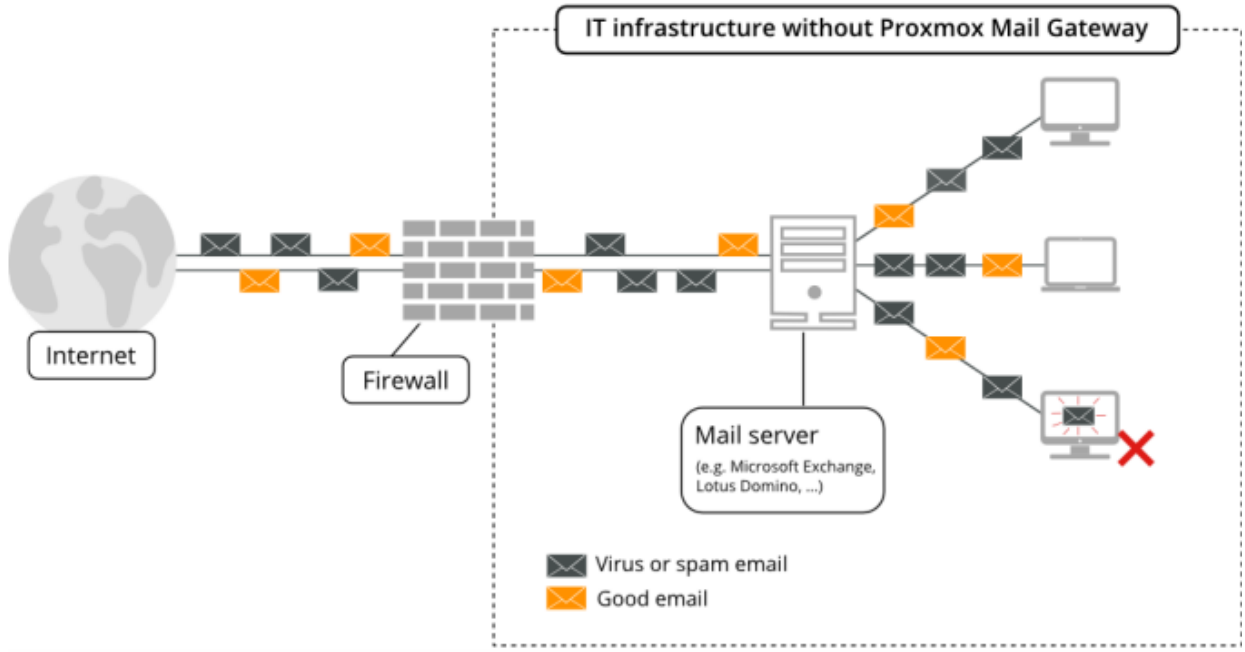
Administrator – пошта сүзгісін теңшеуге толық қол жеткізу, бірақ желі параметрлерін өзгертуге рұқсат етілмейді.

Quarantine Manager – спам-карантинді қарау және басқару мүмкіндігі болып табылады.

Auditor – тек барлық конфигурациялы оқу үшін қол жетімді, журналдарға қол жеткізе алады және статистиканы көре алады.

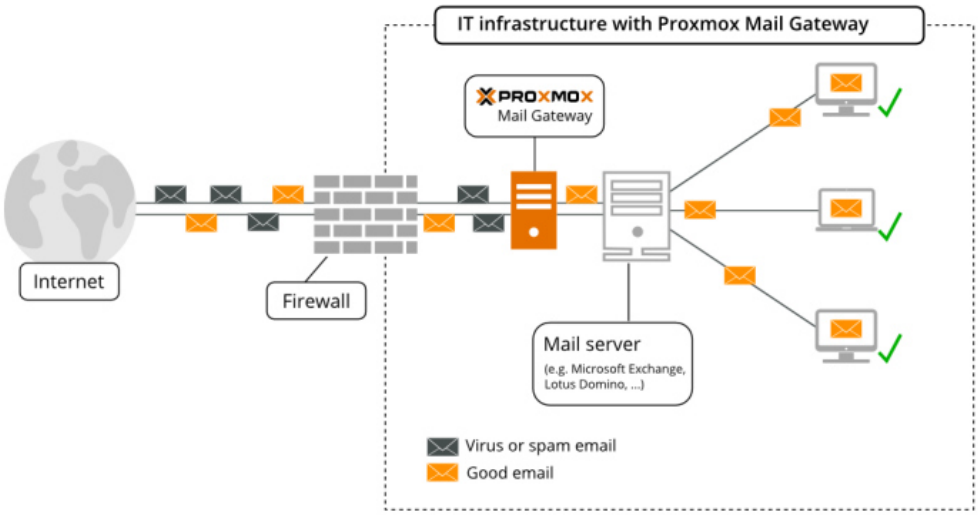
3.4 Қондырылуды жоспарлау

Электрондық пошта серверінің қолданыстағы архитектурасына қарапайым интеграция. Бұл мысалда электрондық пошта трафигі (SMTP) брандмауэрге келіп, электрондық пошта серверіне тікелей жіберіледі.



Сурет 3.2 – Пошта серверінің шлюзбен қоршалуы

Proxmox пошта шлюзінің көмегімен барлық пошта трафигі барлық пошта трафигін сүзетін және қалаусыз хабарламаларды жоятын 3.3 суреттегі Proxmox пошта шлюзіне жіберіледі. Кіріс және шығыс пошта трафигін басқара ала отырып, 3.3 суреттегідей нәтижеге жету мақсаттанады.



Сурет 3.3 – Пошта өтетін шлюздан кейінгі нәтижесі

1) шығыс электрондық хаттарды фильтрлау

Электрондық поштаны сүзгілеу үшін көптеген шешімдер Шығыс хаттарды сканерлемейді. Бұл Proxmox пошталық шлюзі кіріс және шығыс электрондық хаттарды сканерлеу үшін арналған. Бұл екі негізгі артықшылықтары бар:

– Proxmox пошта шлюзі ішкі хост арқылы жіберілген вирустарды анықтауға қабілетті. Көптеген елдерде Сіз вирустарды басқа адамдарға жіберу үшін жауапты боласыз. Proxmox шығыс электрондық пошта шлюзін сканерлеу функциясы Бұл болдырмау үшін қосымша қорғау болып табылады.

– Proxmox пошта шлюзі шығыс электрондық хаттар туралы статистиканы жинай алады. Кіріс хаттар туралы Статистика жақсы көрінеді, бірақ олар мүлдем пайдасыз. Екі пайдаланушыны қарастырайық, user - 1 жаңалықтар порталынан 10 хат алады және сіз ешқашан естімеген адамға 1 хат жазды. 2 пайдаланушы клиенттен 5 хат алады және кері 5 хабарлама жіберді. Қандай пайдаланушы Белсенді деп санайсыз? Мен пайдаланушылар-2, өйткені ол сіздің клиенттеріңізбен сөйлеседі. Proxmox Mail Gateway advanced address статистика бұл маңызды ақпаратты көрсете алады. Шығыс электрондық поштаны сканерлемейтін шешім мұны жасай алмайды.

3.5 Брандмауэр параметрлері

Шығыс HTTP байланысы негізінен вирусты үлгілердің жаңартуларымен пайдаланылады және интернетке тікелей қосудың орнына прокси серверді пайдалануға болады (Кесте 3.1).

Шығыс поштаны сүзуді қосу үшін, сіз жай ғана барлық шығыс "smarthost" пошта серверіне жіберу керек.

Proxmox пошта шлюзі Debian негізделген және толық Debian жүйе, сондай-ақ Proxmox пошта шлюзінің барлық қажетті пакеттері[8].

Орнатушы сізге бірнеше сұрақ қояды, содан кейін жергілікті дискіні(дискілерді) сындырады, барлық қажетті пакеттерді орнатады және

базалық желілік қондырғыны қоса алғанда, жүйені реттейді. Сіз бірнеше минут ішінде толық функционалдық жүйені ала аласыз. Бұл орнатудың қолайлы және ұсынылатын тәсілі.

Кесте 3.1 – Брадмауерға қойылатын ережелер параметрлері

Сервис	Порт	Протокол	Кімнен	Кімге
SMTP	25	TCP	PROXMOX	INTERNET
SMTP	25	TCP	INTERNET	PROXMOX
SMTP	26	TCP	MAILSERVER	PROXMOX
NTP	123	TCP/UDP	PROXMOX	INTERNET
RAZOR	2703	TCP	PROXMOX	INTERNET
DNS	53	TCP/UDP	PROXMOX	DNS SERVER
HTTP	80	TCP	PROXMOX	INTERNET
GUI/API	8006	TCP	INTERNET	PROXMOX

3.6Жүйеге қойылатын талаптар

Proxmox пошталық шлюзі бөлінген серверлік жабдықта немесе виртуалды машинаның ішінде платформа формасының кез келгенінде жұмыс істей алады:

- Proxmox VE (KVM);
- VMWare vSphere™ ;
- Hyper-V™ ;
- KVM ;
- Virtual box™;
- Citrix Hypervisor™;
- LXC container.

Жүйелікталаптар

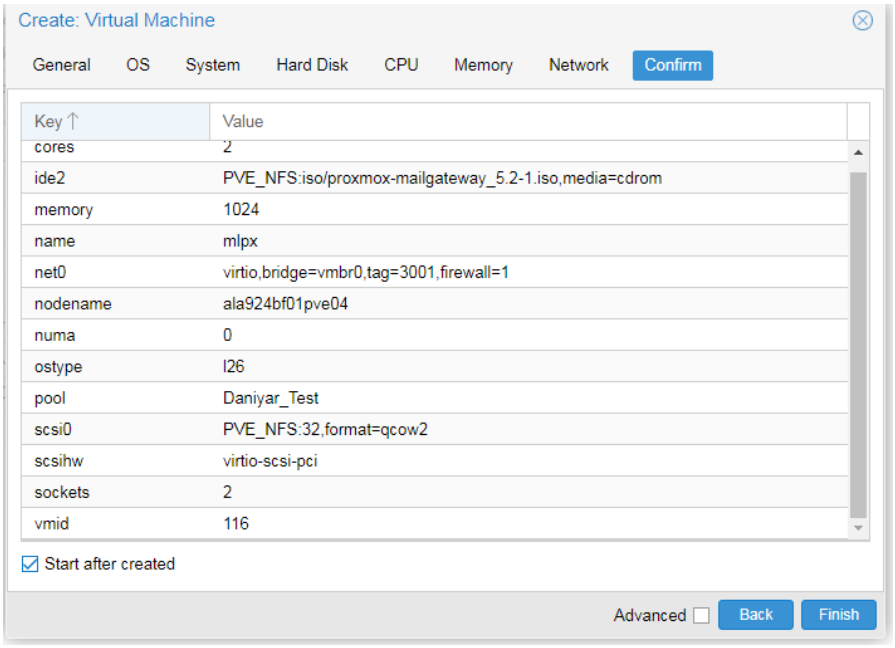
- ЦПУ: 64bit (Intel EMT64 немесе AMD64);
- ГБ ОЗУ
- USBқолдану
- кем дегенде 8 ГБ диск кеңістігі бар қатты диск
- ethernet желілік картасы

3.7Бағдарлама жұмысы

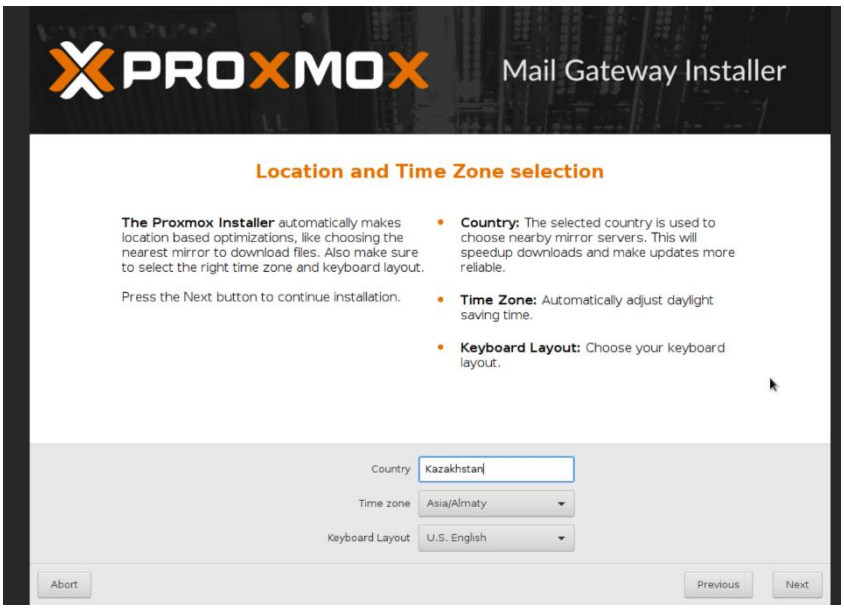
Сонымен қатар, Proxmox пошталық шлюзін қолданыстағы Debian жүйесінің үстінен орнатуға болады. Бұл параметр тек тәжірибелі пайдаланушылар үшін ұсынылады, өйткені ол Proxmox және Debian пошта шлюзі туралы толығырақ білімді қажет етеді.

1) Proxmox пошта шлюзінің USB-флеш дискісі арқылы орнату.

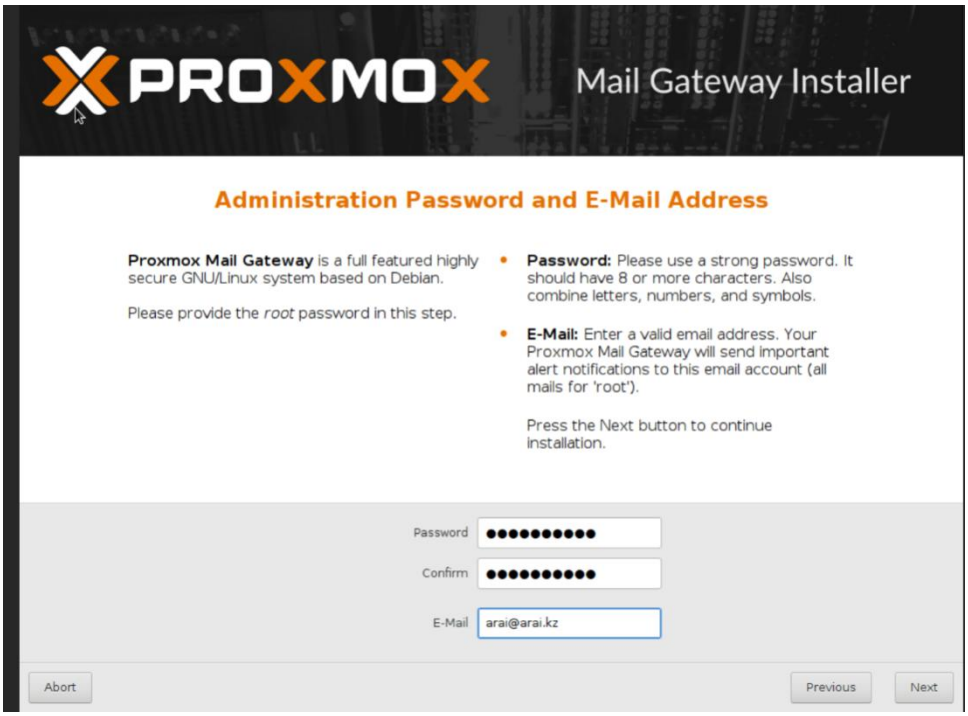
Сурет 3.4 – Бастапқы қарсалу кестесі



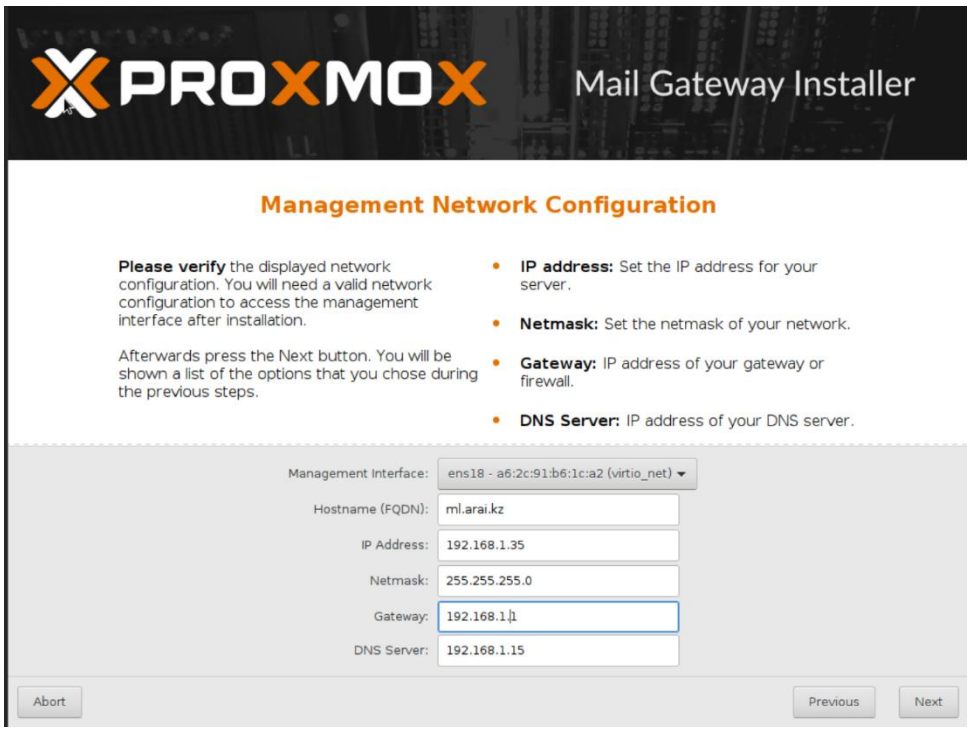
Сурет3.5 – Сервер конфигурациялары



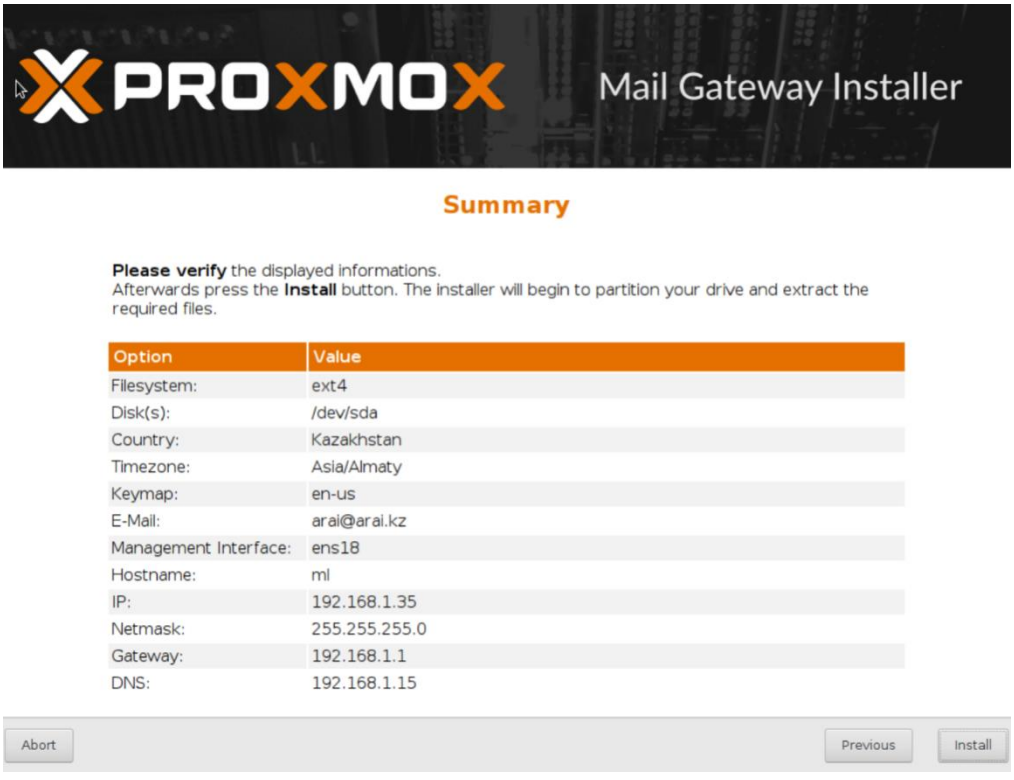
Сурет 3.6 – Серверде ел таңдауы



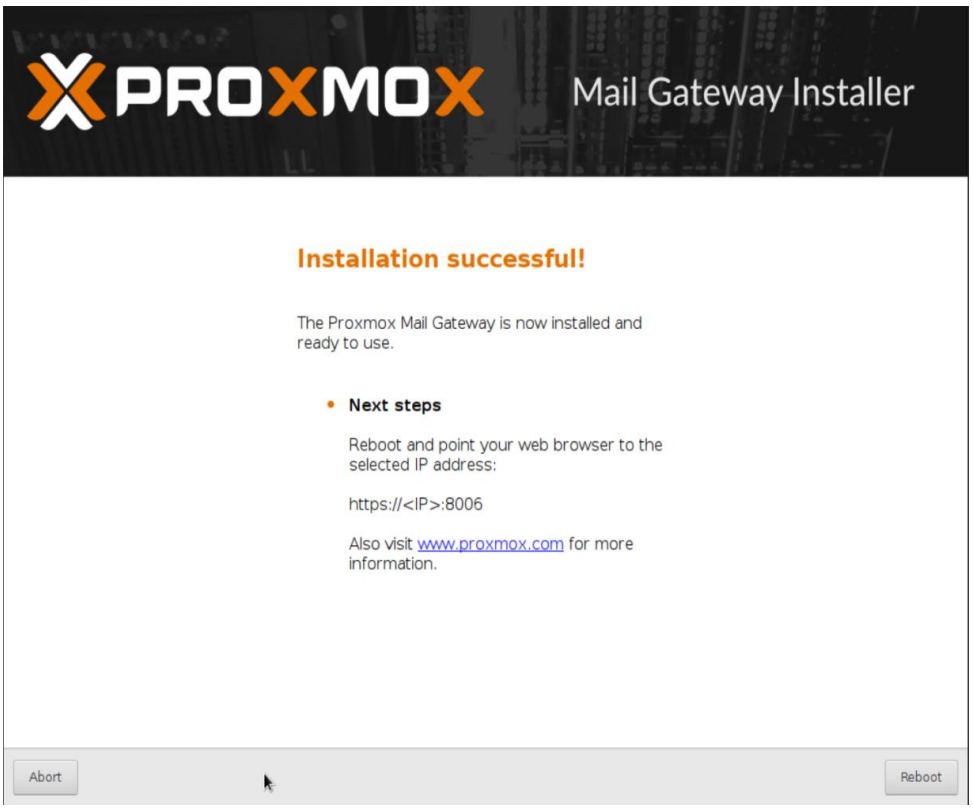
Сурет 3.7 – Сервердің кіру құжаттары



Сурет 3.8 – Трафик өтетін интерфейсті қою

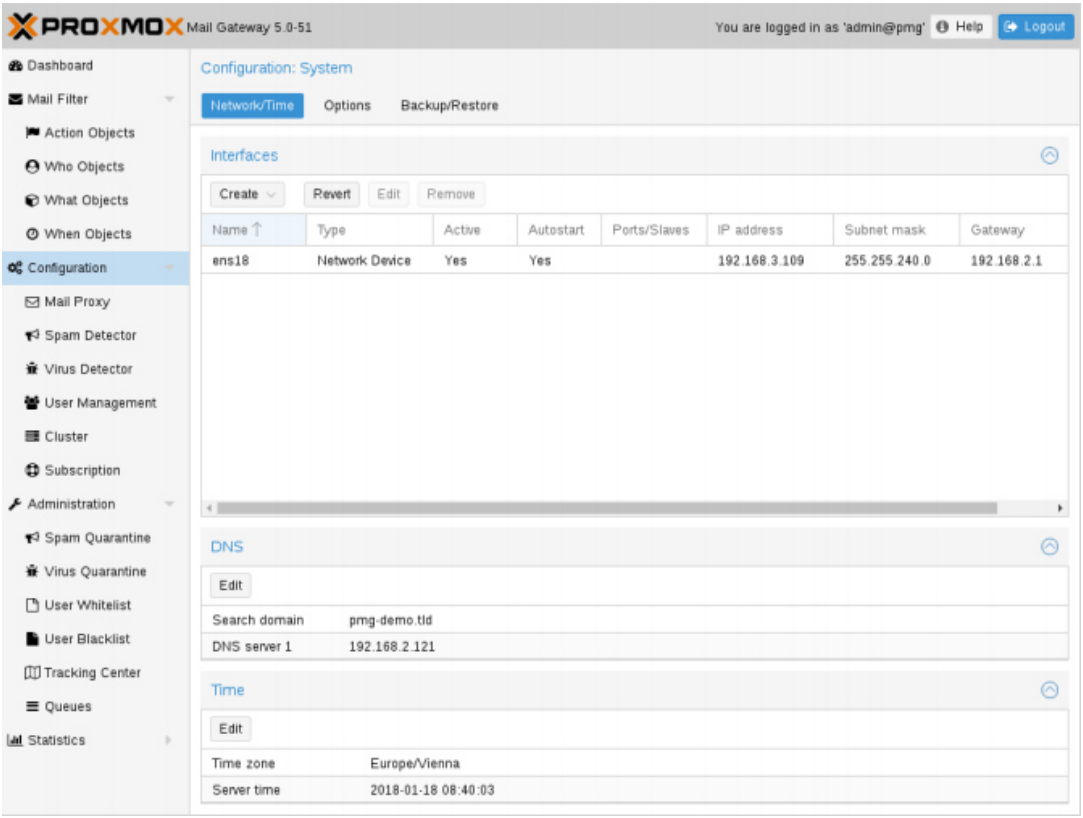


Сурет 3.9 – Қорытынды тізім



Сурет 3.10 – Қайта қосу ескертуі

Әдетте 3.11 суреттегі GUI-ге барған кезде желі мен уақыт теңшелген. Орнатушы осы параметрлерді сұратады және дұрыс мәндерді орнатады. Әдетте бір Ethernetадаптері және IP статикалық мақсаты қолданылады. Конфигурация /etc/network / interfaces-те сақталады, ал желіні нақты баптау ifupdown бумасы арқылы Debian стандартты тәсілмен орындалады.

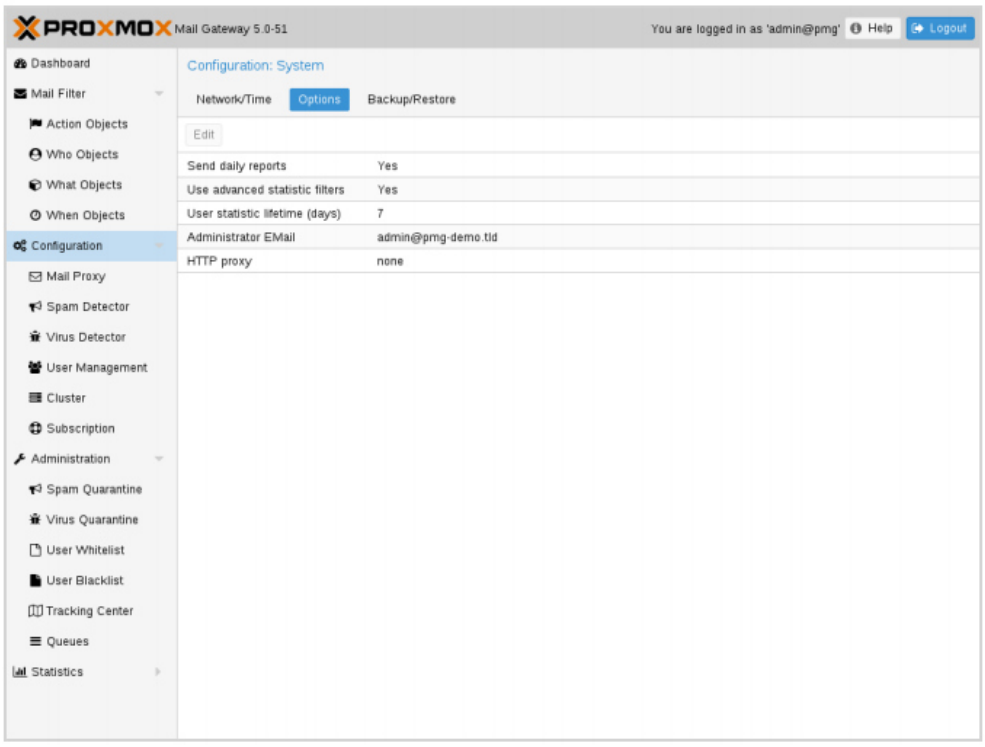


Сурет 3.11– Бастапқы беті

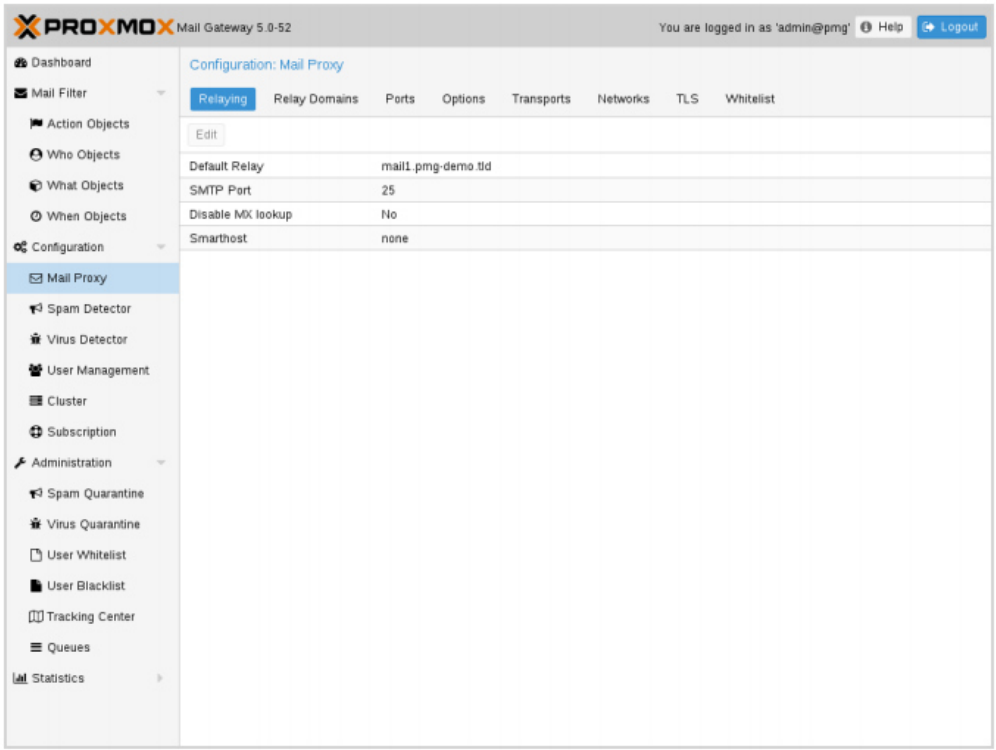
DNS ұсынысы

Спам анықтау үшін көптеген тесттер DNS-сұрауларды пайдаланады, сондықтан жылдам және сенімді DNS-сервері болуы маңызды. Біз сондай-ақ кейбір ортақ қара DNS тізімін сұраймыз. Олардың көпшілігі клиенттер үшін жылдамдықты шектеуді қолданады, сондықтан олар жай ғана жұмыс істемейді, егер сіз жалпы DNS-серверді пайдалансаңыз (олар әдетте бұғатталады, өйткені). Рекурсивті режимде теңшеу қажет жеке DNS-серверді пайдалану ұсынылады.

Сурет 3.12-гі параметрлер /etc/pmg/pmg файлындағы admin бөлімшесінде сақталады.

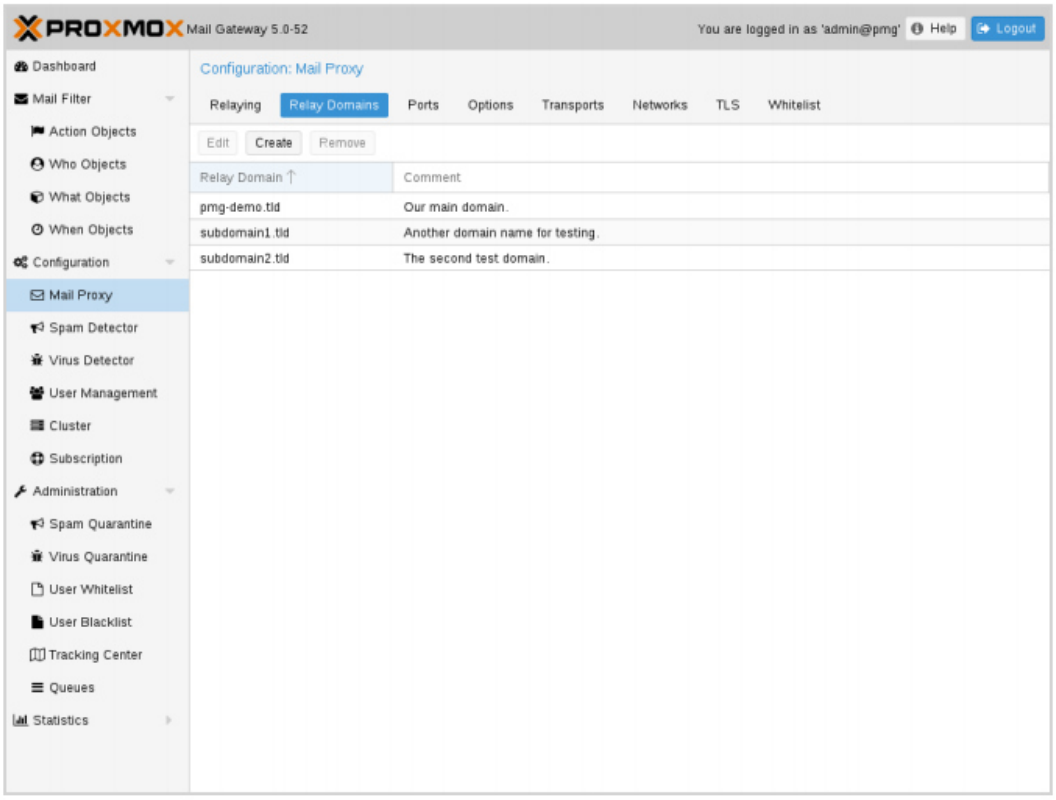


Сурет 3.12 – Бірінші конфигурация тізімі

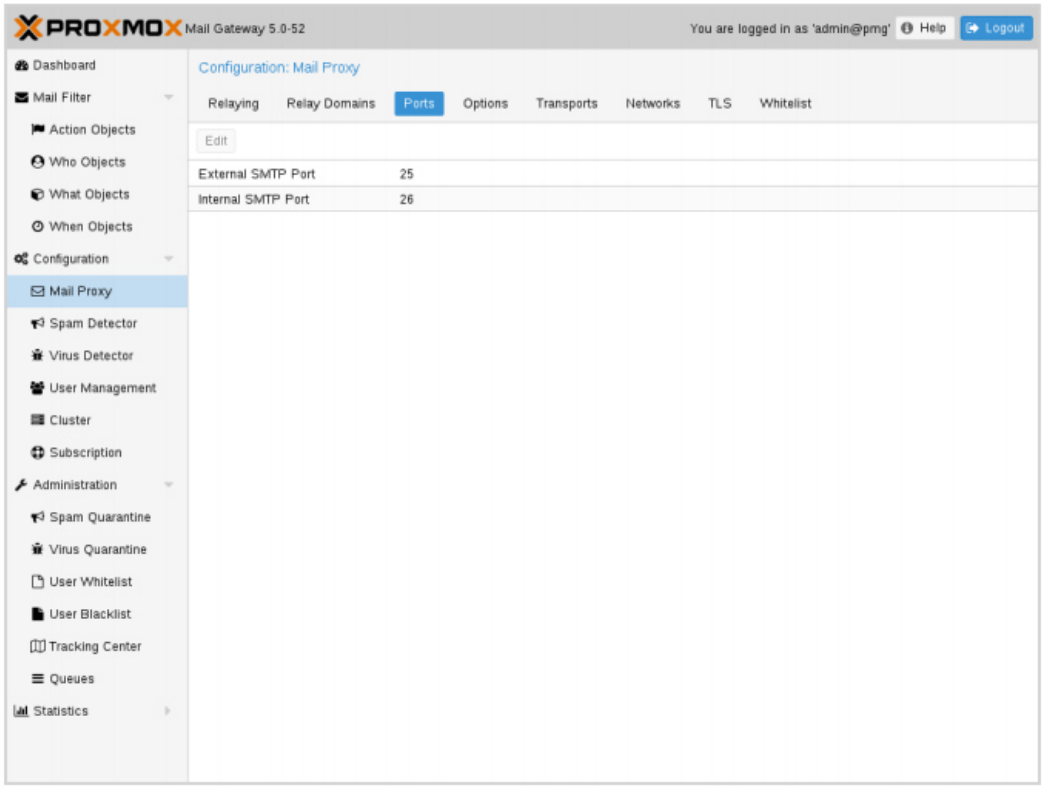


Сурет 3.13 – Пошта прокси жіктеу

Сурет 3.14 –гі ретрансляторлық почта домендер, пошта басқа домен арқылы жіберілетінің баптауы. Жүйе кіріс хабарларды басқа домендерге қабылдамайды.

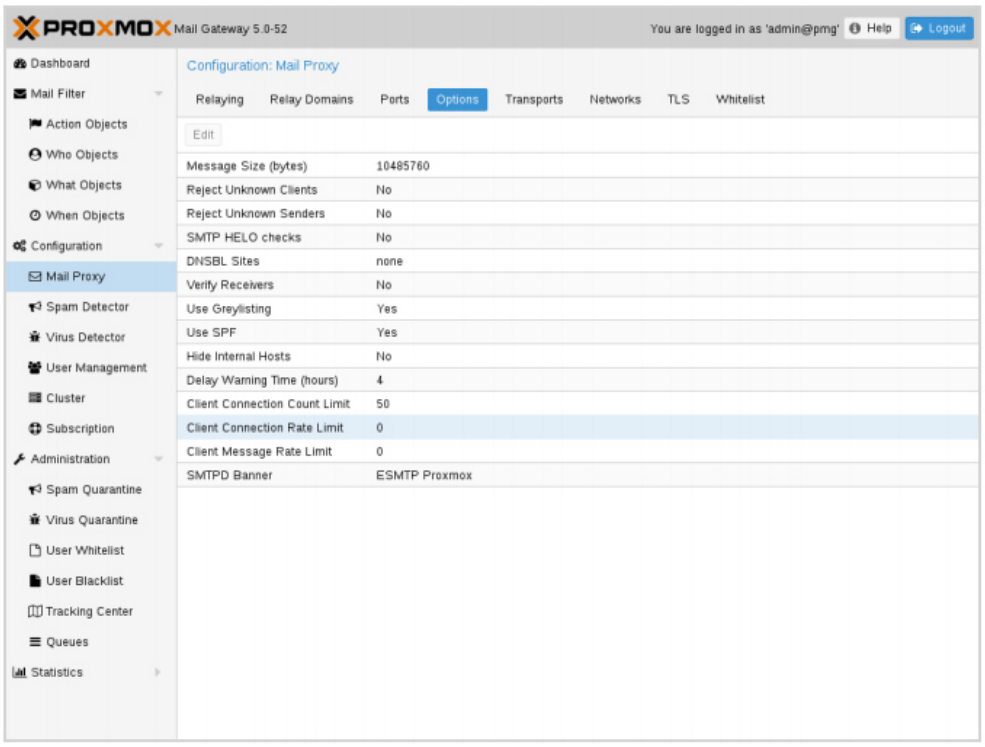


Сурет 3.14 – Пошта проксисіңРесей доменін жолдауы

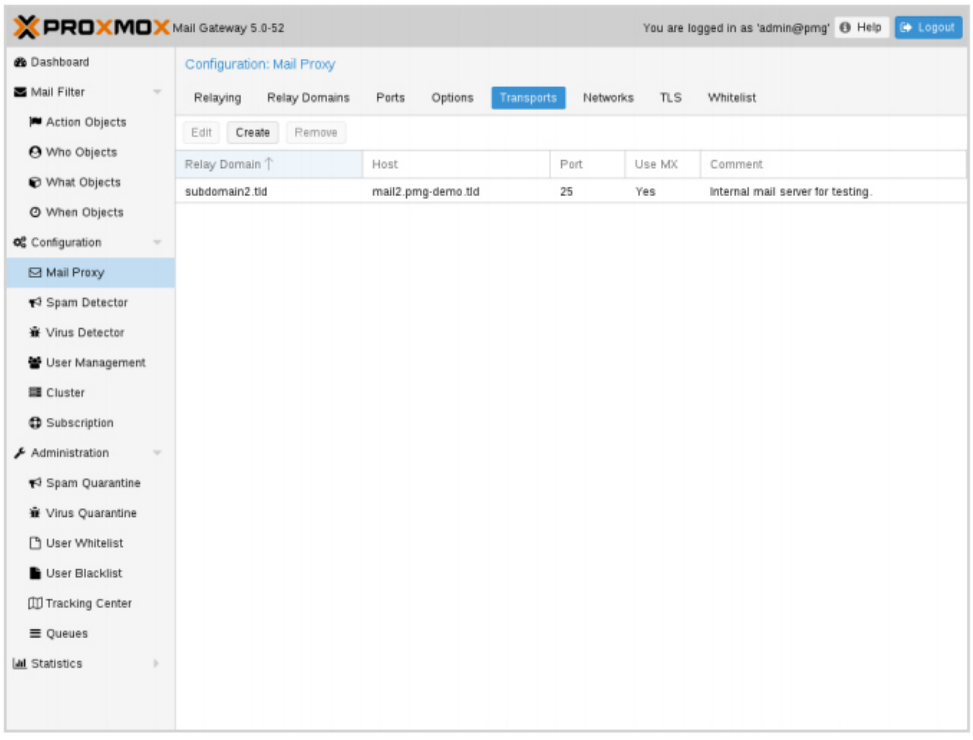


Сурет 3.15 – Порттарды жіктеу

Сурет 3.16параметрлер /etc/pmg / pmg пошта бөлімшесінде сақталады.



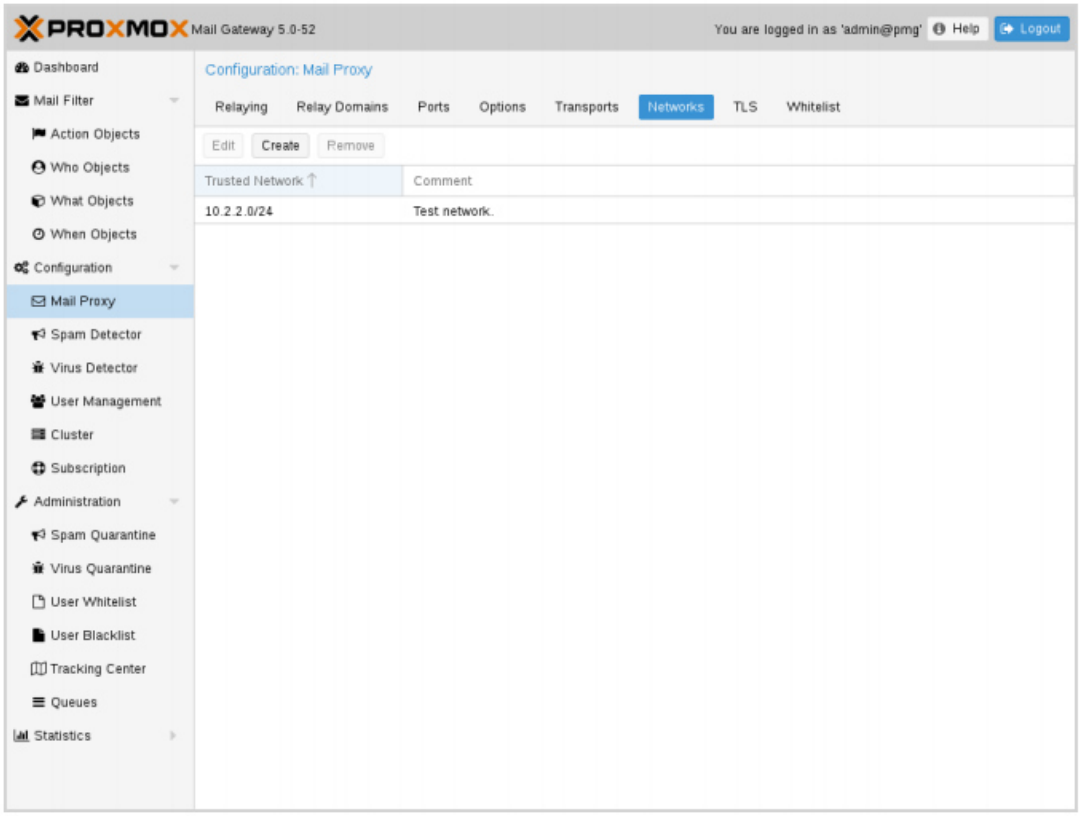
Сурет 3.16 – Пошта прокси жіктеме бөлімі



Сурет 3.17 – Бастапқы қарсалу кестесі

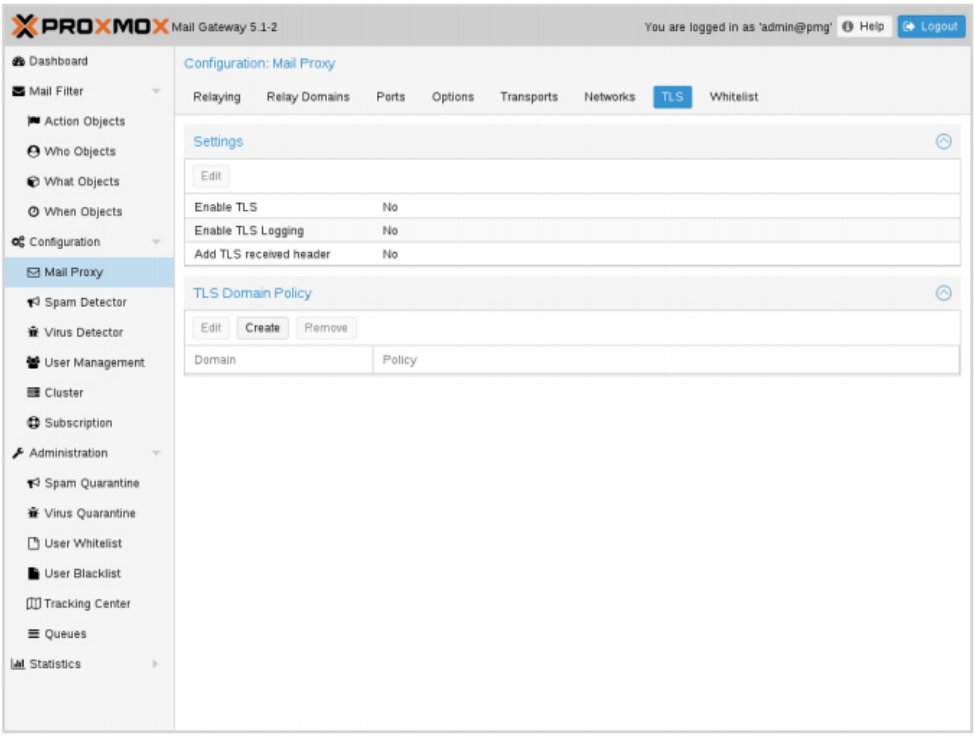
Proxmox пошта шлюзін түрлі ішкі пошта серверлеріне электрондық поштаны жіберу үшін пайдалануға болады. Мысалы, электрондық хаттарды жіберуге болады domain.com сіздің бірінші пошта серверіне және жіберілген хаттар subdomain.domain.com екінші үшін. (сурет 3.17)

Қосымша пошта серверлерінің IP адрестерін, хост атын, SMTP порттарын және пошта домендерін (немесе тек жеке электрондық пошта адрестерін) қосуға болады.



Сурет 3.18– Тікелей шетел проксиді жіктеу

Қосымша ішкі (сенімді) IP желісі немесе хосты қосуға болады. Бұл тізімдегі барлық хост қайта таратуға болады.



Сурет 3.19 – TLS жіктеу

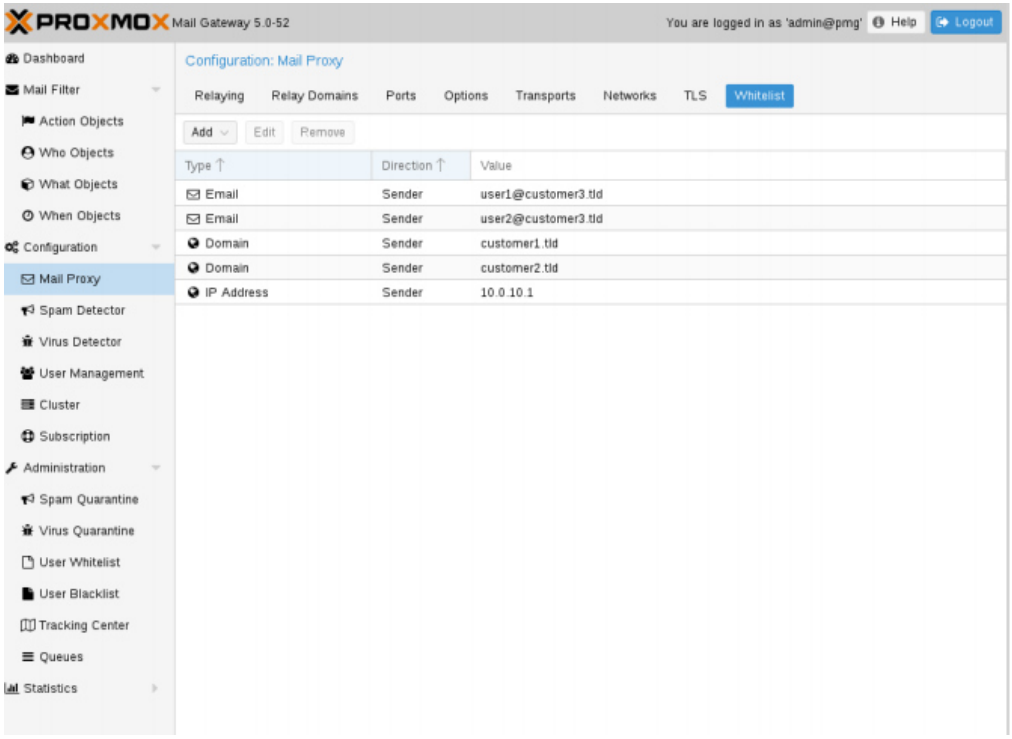
Transport Layer Security (Сурет 3.19) сертификаттардың және шифрланған сеанстардың негізінде түпнұсқалығын тексеруді қамтамасыз етеді. Шифрланған сеанс SMTP поштасы арқылы берілетін ақпаратты қорғайды. TLS іске қосылған кезде Proxmox пошта шлюзі автоматты түрде сіз үшін жаңа өздігінен растаушы сертификатты жасайды.

TLS журналын жүргізуді қосу

SMTP TLS қызметі туралы қосымша ақпарат алу үшін TLS журналын жүргізуді қосуға болады. Осылайша, TLS сеанстары және қолданылатын сертификат туралы ақпарат syslog арқылы тіркеледі.

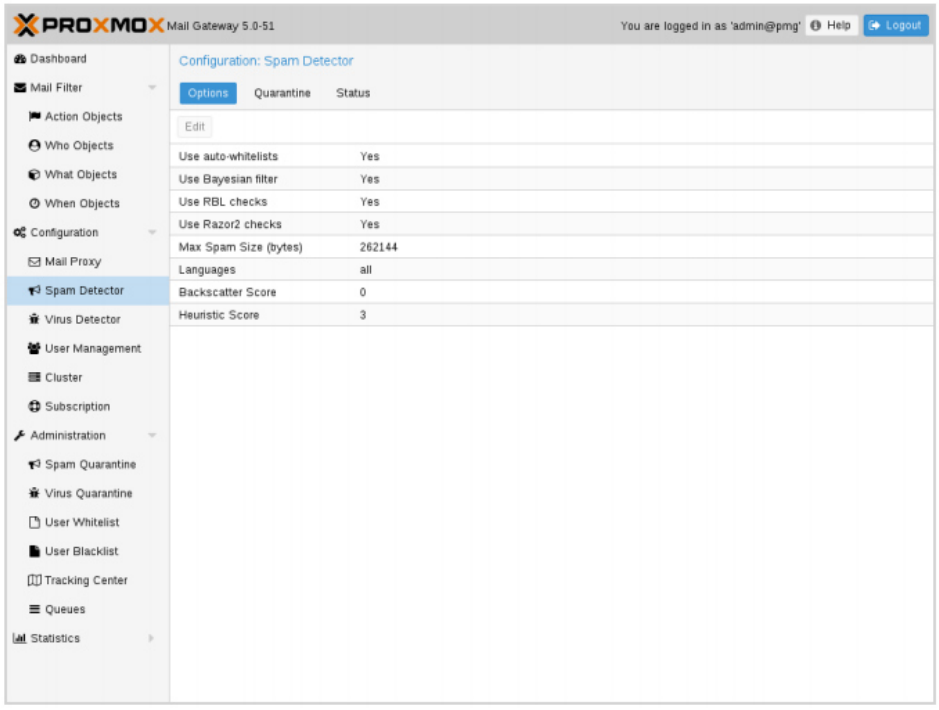
Алынған TLS тақырыбын қосу

Қолданылатын хаттама мен Шифр, сондай-ақ клиенттің және Эмитенттің аты туралы ақпаратты хабарлама.



Сурет 3.20 – АҚ листі бөлімі

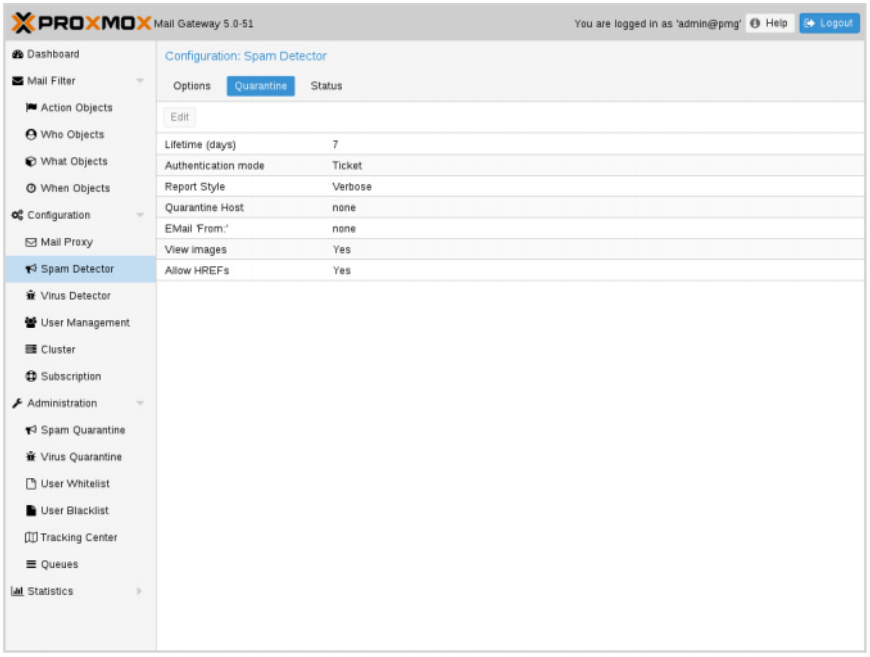
Сурет 3.21-дегі жазбалар үшін барлық SMTP тексеру өшірілді



Сурет 3.21 – Спам детектрлеу

Proxmox пошта шлюзі спам сигналдарын сәйкестендіру үшін жергілікті және желілік тесттердің кең спектрін пайдаланады. 3.22 суреттегі спамерлер үшін бір аспектіні сәйкестендіру қиын, олар спам сүзгі айналасында жұмыс істеу үшін өз хабарлар жасай алады.

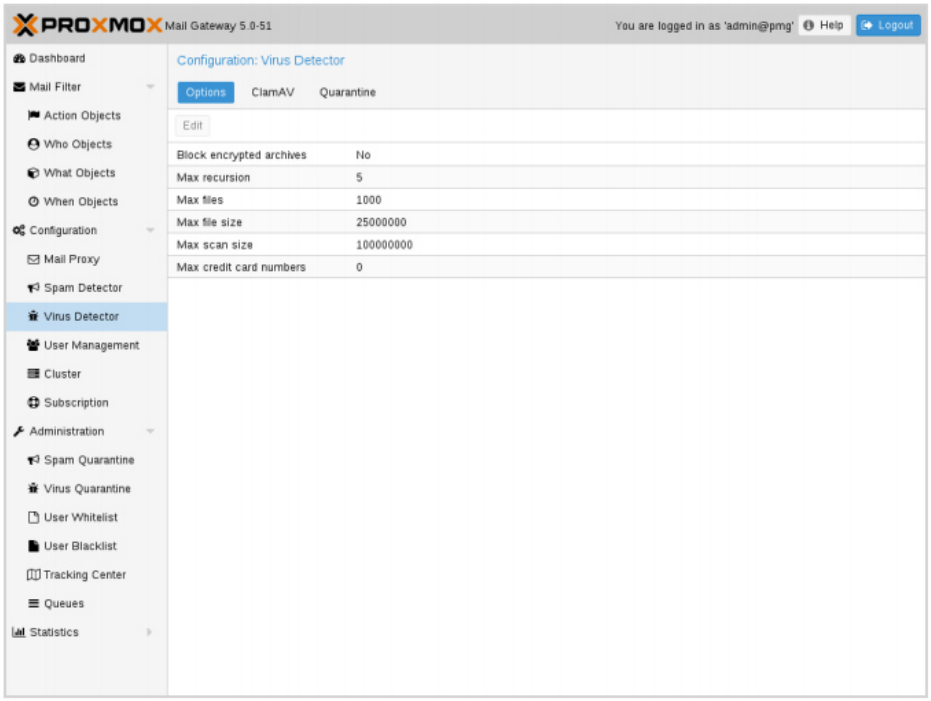
Әрбір электрондық хат талданады және спам бағасын алады. Жүйе жалған іске қосу мен жалған негативтердің санын азайту тұрғысынан орындалатын ережелердің тиімділігін оңтайландыруға тырысады.



Сурет 3.22– Спам детектрлеуінің жіктелу бөлімі

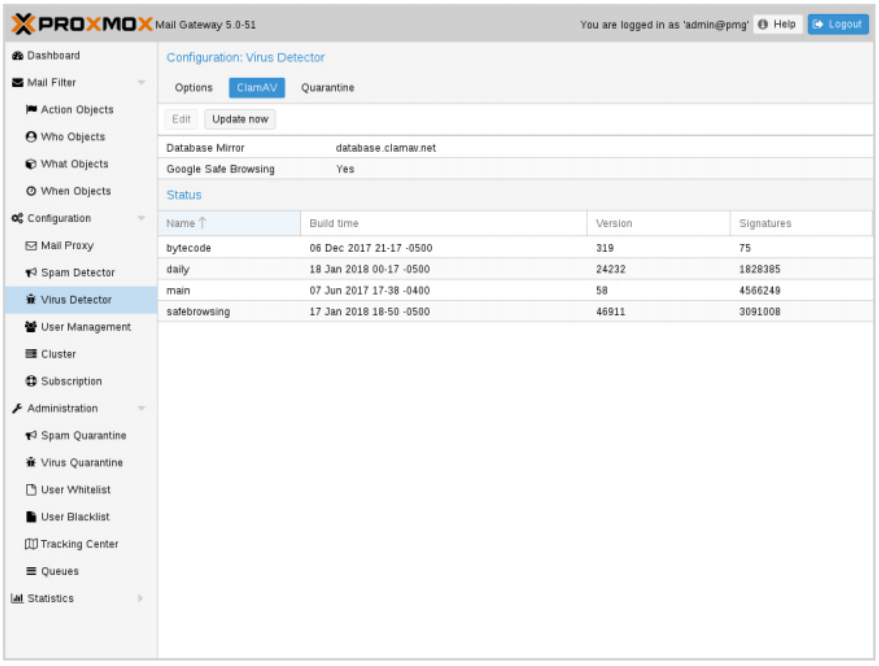
Proxmox барлық кіріс электрондық пошта хаттарын талдайды және оның ветчина немесе спам (немесе вирус) болса, әрбір хат үшін шешеді. Жақсы электрондық хаттар пошта жәшігіне жеткізіледі және спам-хабарламалар карантинге ауыстырылуы мүмкін.

Жүйе пайдаланушыларды соңғы күні алынған жеке спам-хабарламалар туралы хабардар ету үшін күнделікті есептерді жіберуге бапталуы мүмкін. Бұл есеп карантинде жаңа хабарламалар болған жағдайда ғана жіберіледі.



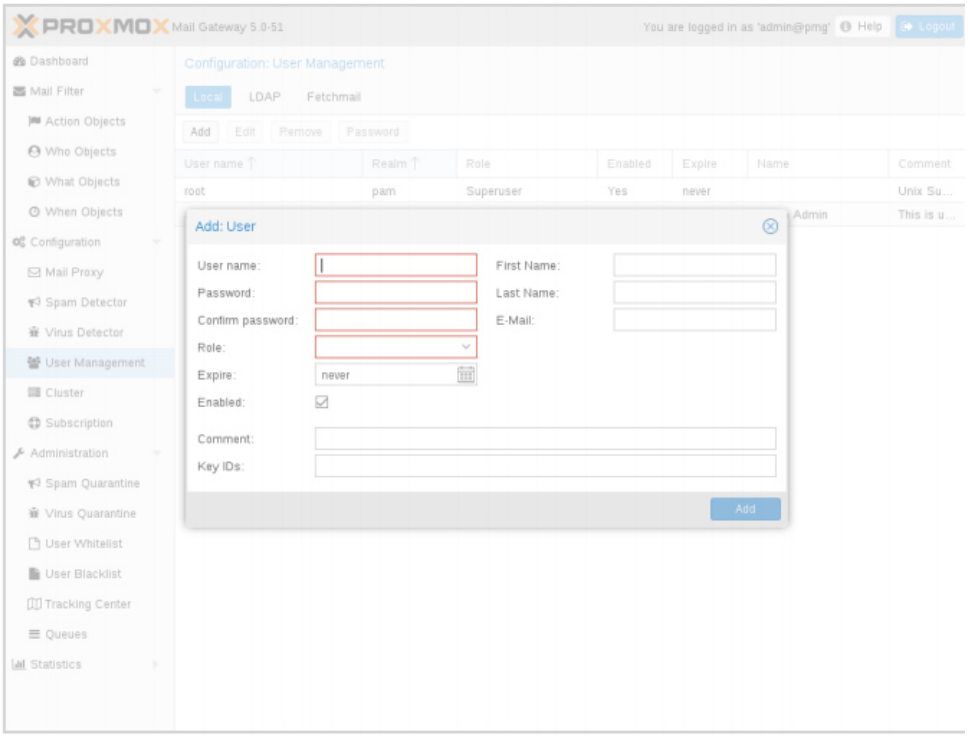
Сурет 3.23 – Вирус детектрі бөлімшесі

Барлық хаттар қосылған вирустар детекторына (Сурет 3.24) автоматты түрде жіберіледі. Әдепкі мән қауіпсіз деп саналады, сондықтан әдетте оларды өзгерту қажет емес.



Сурет 3.25 – ClaimAV антивирус бөлімшесі

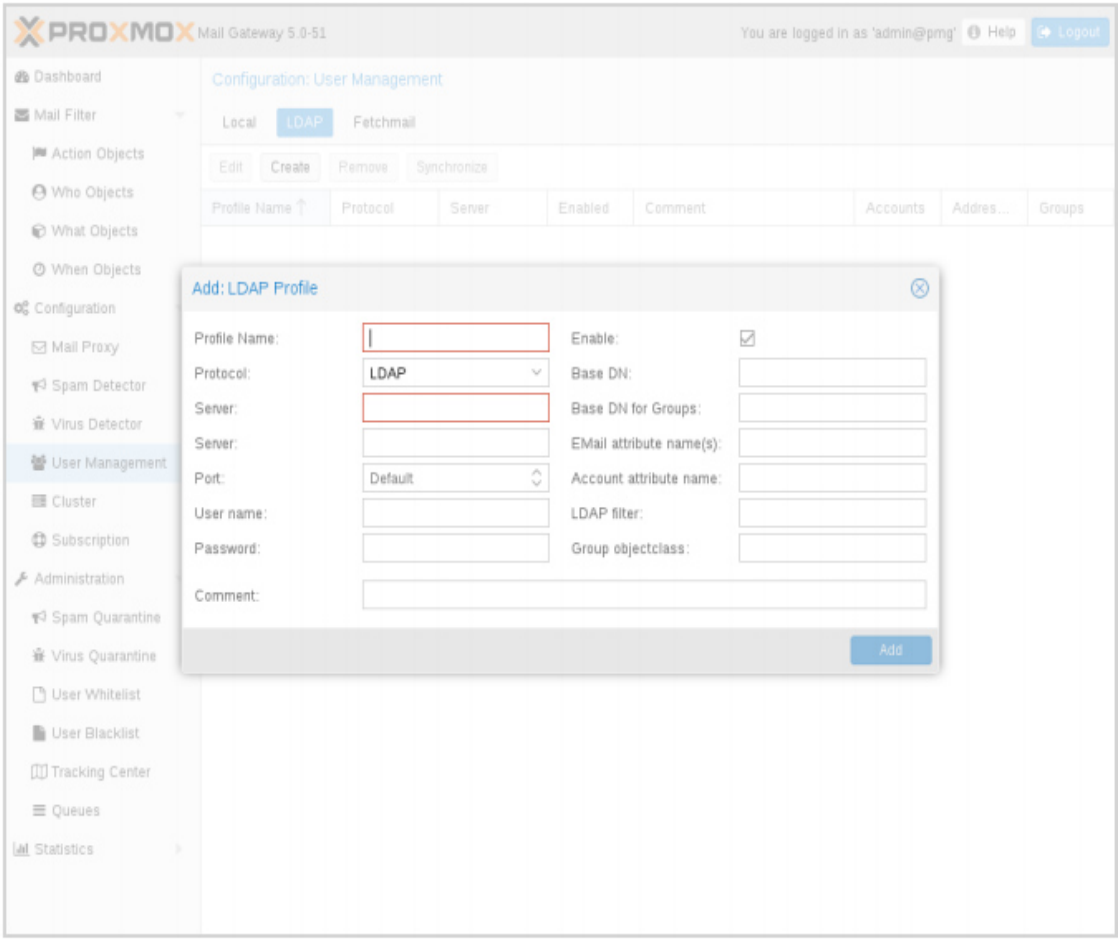
Вирустар сигнатураларының деректер базасы автоматты түрде жаңартылады. Бірақ сіз 3.26 суреттегі GUI деректер қорының күйін көре аласыз, және сіз онда қолмен жаңартуларды іске қосуға болады.



Сурет 3.26–Жергілікті қолданушыны қосі

3.27 суреттегі терезеде жергілікті пайдаланушылар Proxmox пошта шлюзін басқару және аудит үшін пайдаланылады. Бұл пайдаланушылар веб-басқару интерфейсіне кіре алады.

Сонымен қатар, әрдайым хостты жаңарту немесе желі конфигурациясын өзгерту сияқты жүйелік әкімшінің арнайы тапсырмаларын орындау үшін пайдаланылатын root пайдаланушысы бар.



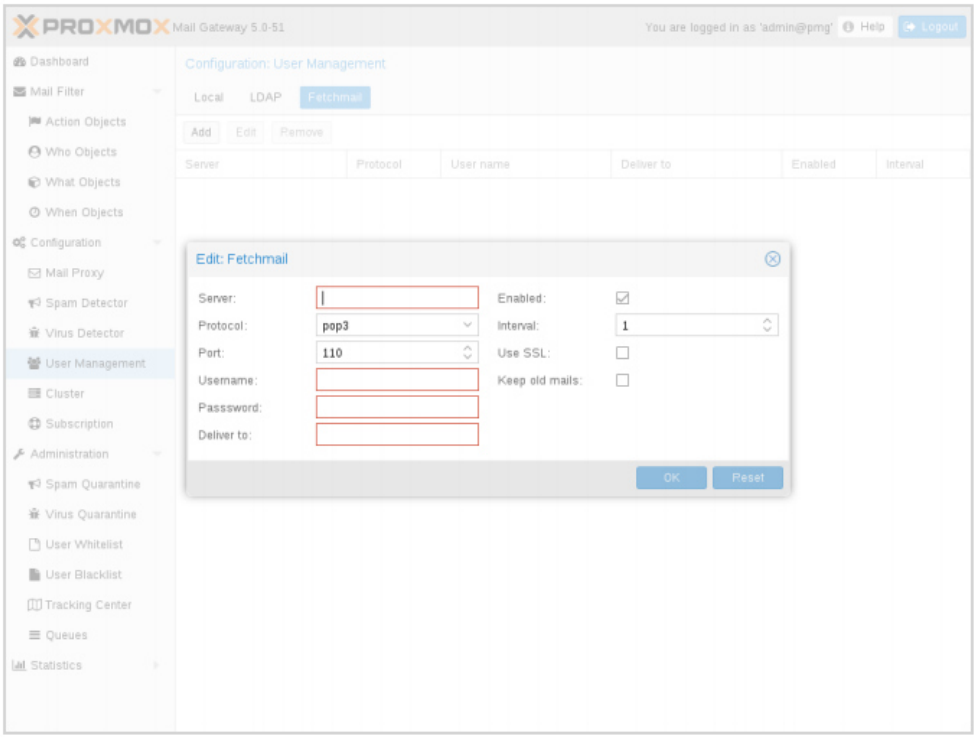
Сурет 3.27–LDAP аутентификациялық қолданушыларды қосу

3.28 суреттегі пайдаланушылар мен топтарға сәйкес ережелерді жасау үшін бірнеше LDAP/Active Directory профильдерін орнатуға болады.

– Профиль жасау үшін келесілер қажет (кем дегенде).
– Профиль атауы.
– Протокол (LDAP немесе LDAPS; ldaps ұсынылады).
– Кем дегенде бір сервер.
– Пайдаланушы және пароль.
– Қадамдастыру.

Proxmox пошта шлюзі LDAP/AD сервері уақытша қол жетімсіз болса да, бұл ақпарат тез қол жетімді болуы үшін пайдаланушы мен топ туралы тиісті ақпаратты мерзімді синхрондайды.

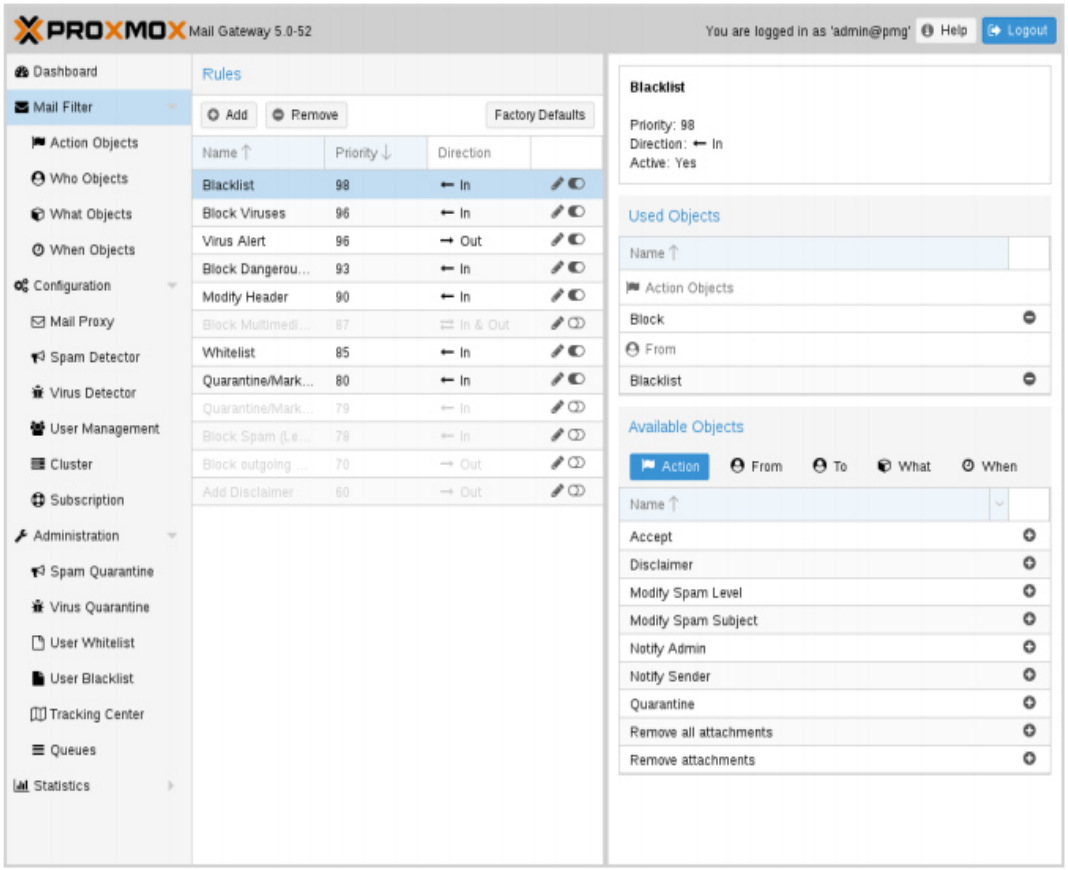
Топ сәтті қадамдастырылғаннан кейін және пайдаланушылар веб-интерфейсте көрінуі тиіс. Осыдан кейін пайдаланушылар мен LDAP топтары үшін ережелер жасауға болады.



Сурет 3.28– Пошта келетін протокол түрі

Fetchmail-сауалнама және электрондық пошта жіберу үшін утилита. Сіз электрондық пошта есептік жазбаларын анықтауға болады, содан кейін сіз көрсеткен электрондық пошта мекенжайына жіберіледі.

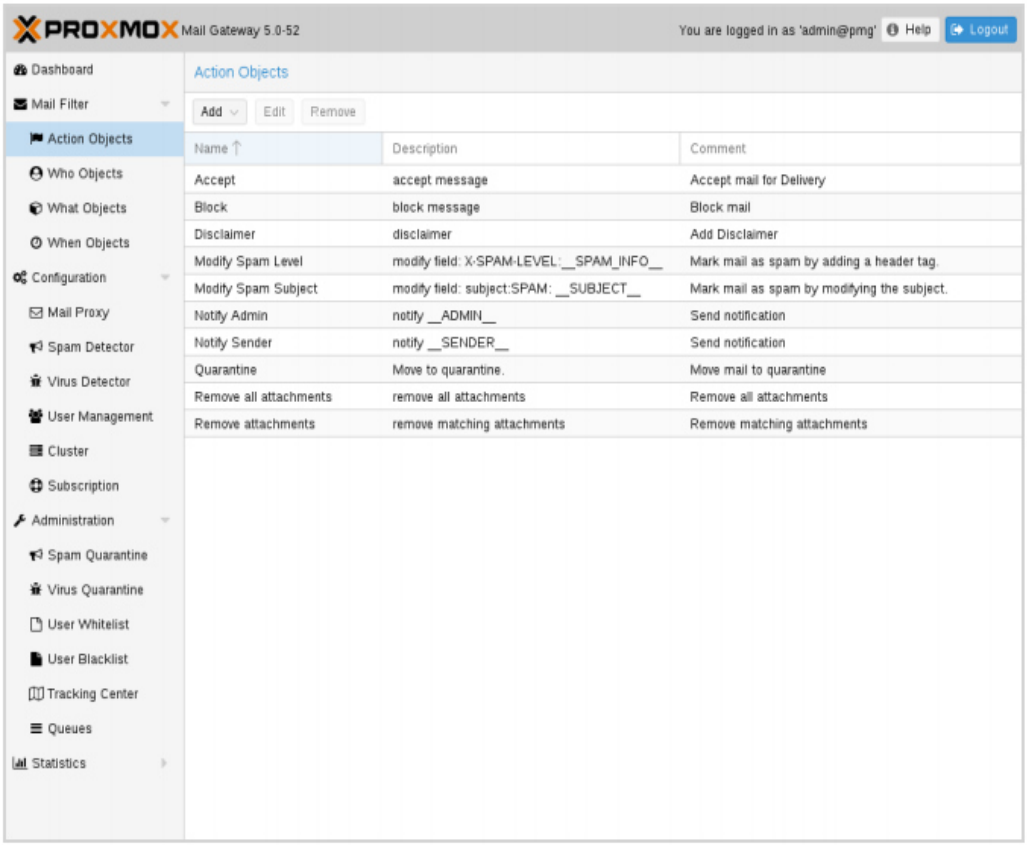
Сіз қосу үшін жазба әрбір шот / мақсаттар, сіз алу және жіберу. Содан кейін олар үнемі сұралып, 3.29суреттегі конфигурацияға сәйкес қайта бағытталатын болады.



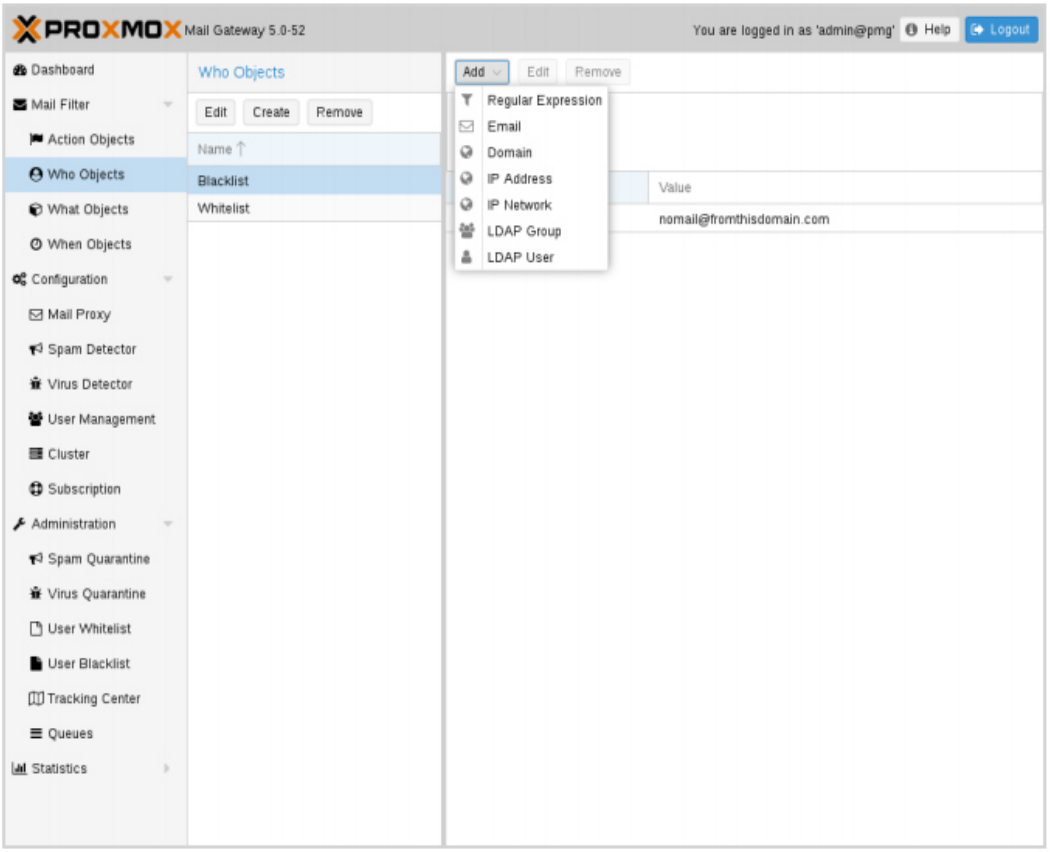
Сурет 3.29 – Пошта сүзгісі

Әрбір ереже 5 санатқа ие (FROM, TO, WHEN, WHAT және ACTION) және әрбір санат белгілі бір критерийлерге сәйкес келетін бірнеше объектілерді қамтуы мүмкін.

Карантинге жылжыту (вирустық хаттар "вирустардың карантиніне" ауыстырылады, басқа хаттар"спам карантіне"ауыстырылады). 3.30 суретте қорытынды әрекет бапталады.

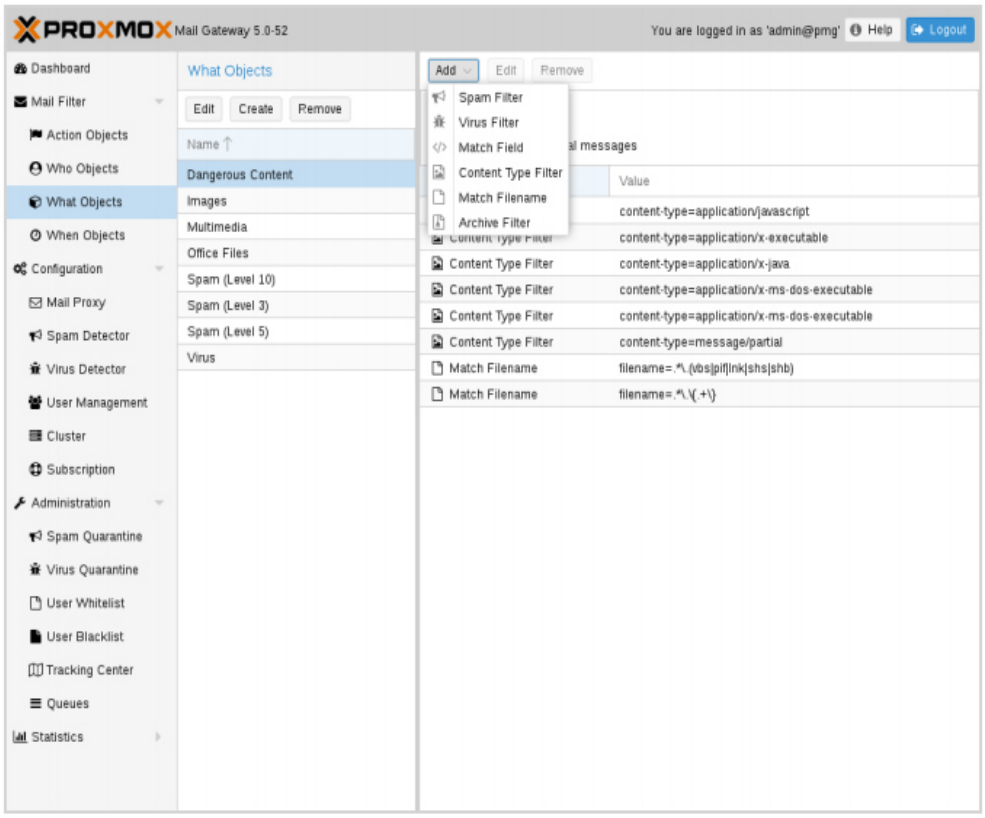


Сурет 3.30 – ACTION объект ереже бөлімшесі



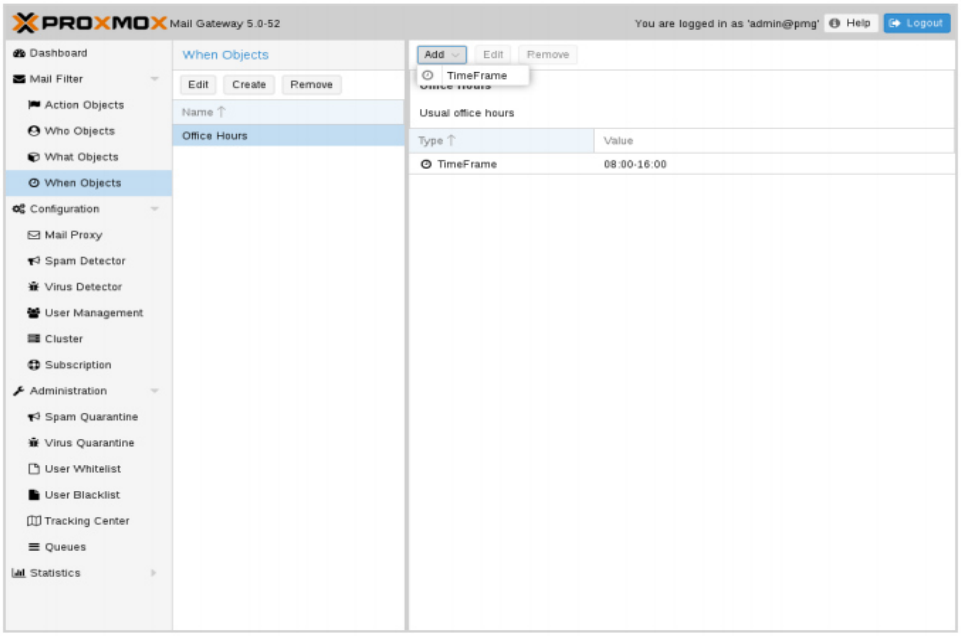
Сурет 3.31 – WHILEобъект ереже бөлімшесі

3.32 суреттегі нысандар түрі кімге және/немесе до, ал macth жіберушісі немесе электрондық пошта алушы санатына пайдаланылуы мүмкін. Бір нысан бірнеше элементтерді біріктіре алады және келесі элементтерді қол жетімді:



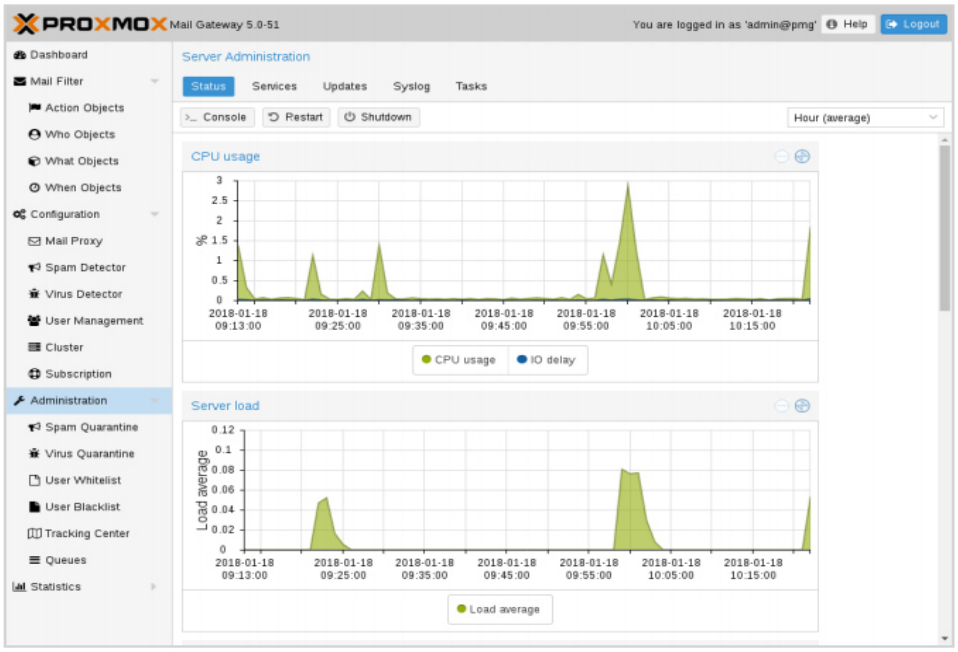
Сурет 3.32 – WHAT объект ереже бөлімшесі

Хабар мазмұнын 3.33 суреттегідей жіктеу үшін қандай нысандар пайдаланылады. Бір нысан бірнеше элементтерді біріктіре алады және келесі элементтерді қол жетімді:



Сурет 3.33–WHEN объект ереже бөлімшесі

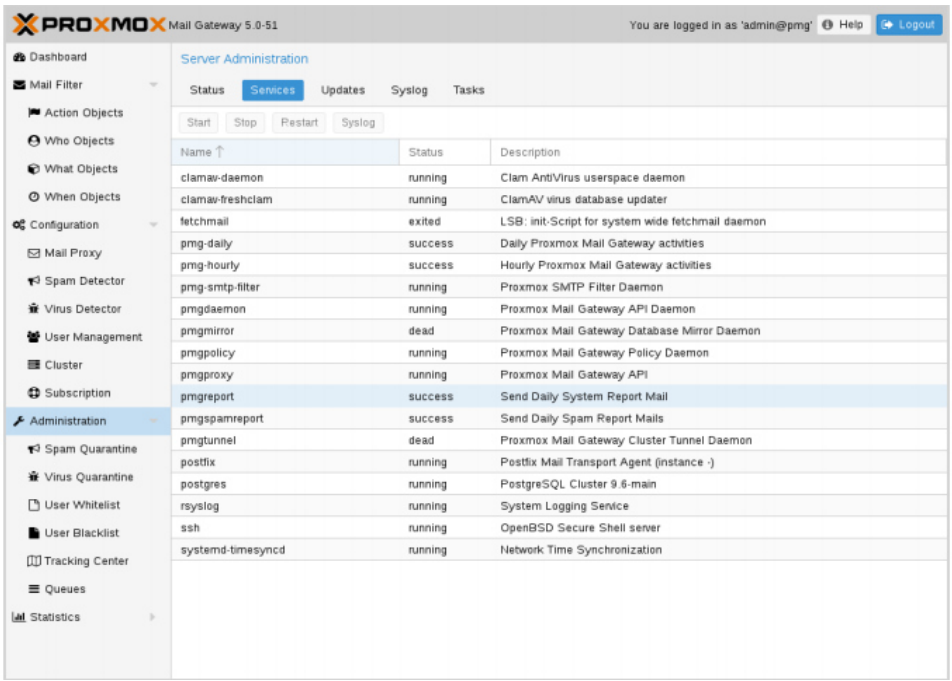
3.34 суретте нысандар ережелерді тәуліктің белгілі бір уақытында іске қосу үшін пайдаланылады. Сіз оларды бір немесе бірнеше таймфрейм элементтерінен жасай аласыз.



Сурет 3.34 – Администраторлық мониторинг жүйесінің бөлімшесі

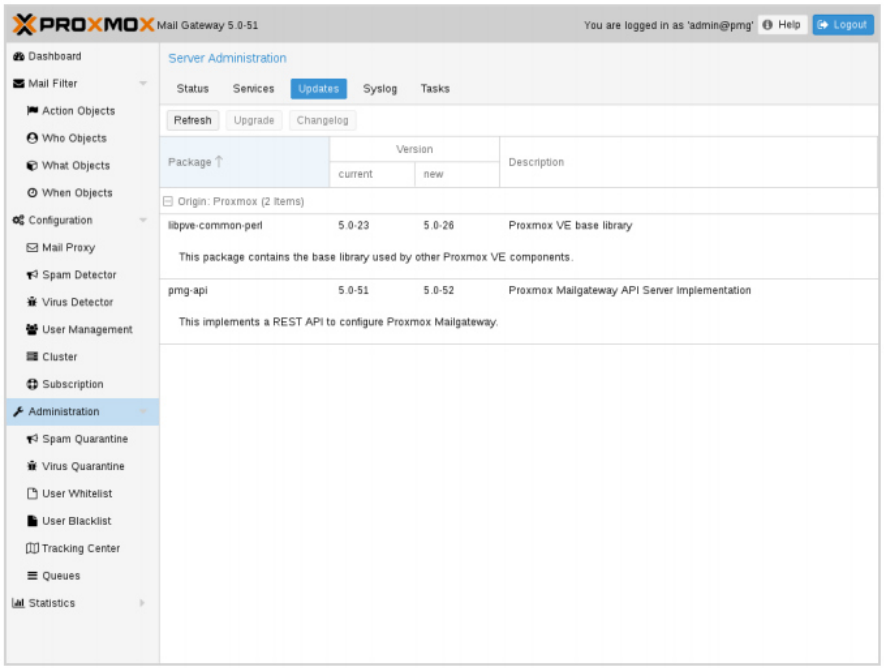
3.35 суреттегі бет сервердің БҚ, жады, диск және желіні пайдалану статистикасын көрсетеді. Жоғарғы оң жақ бұрышында көрсетілетін уақыт аралығын таңдай аласыз.

Әкімшілер консоль түймесі арқылы терминал терезесін аша алады. Сондай-ақ, серверді қайта іске қосуға немесе аяқтауға болады.



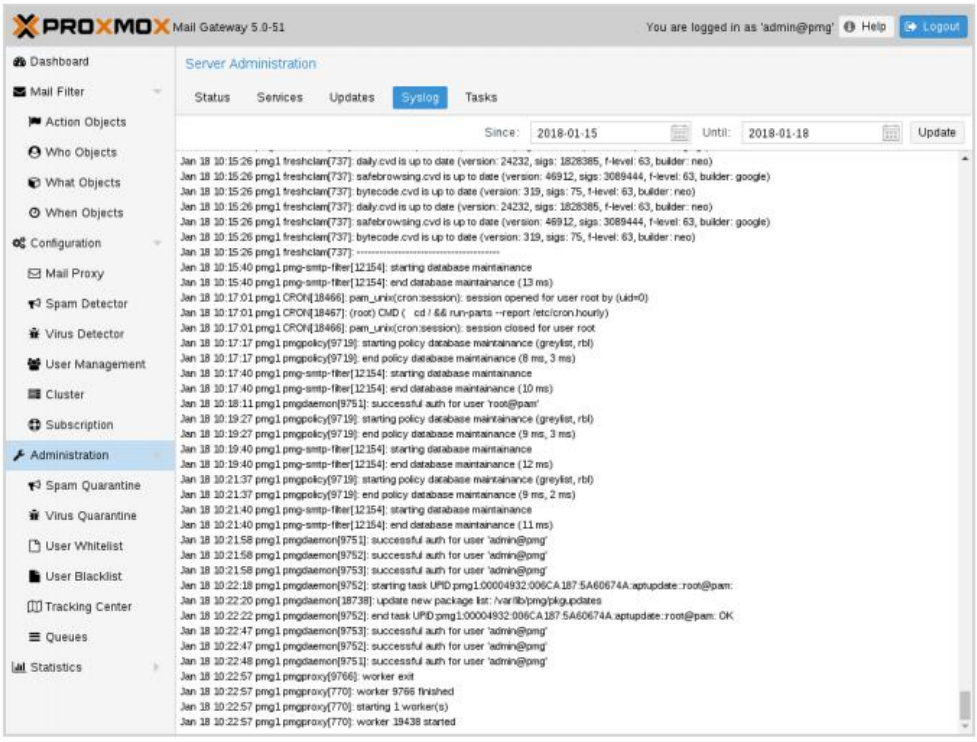
Сурет 3.35 – Администраторлық сервистер бөлімшесі

3.36 суреттегі панельде поштаны өңдеу және кластерлерді синхрондау үшін пайдаланылатын барлық негізгі қызметтер көрсетілген. Қажет болған жағдайда, сіз оларды іске қосу, тоқтату немесе қайта іске қосу мүмкін. Syslog түймесі таңдалған қызметке сүзілген жүйелік журналды көрсетеді.



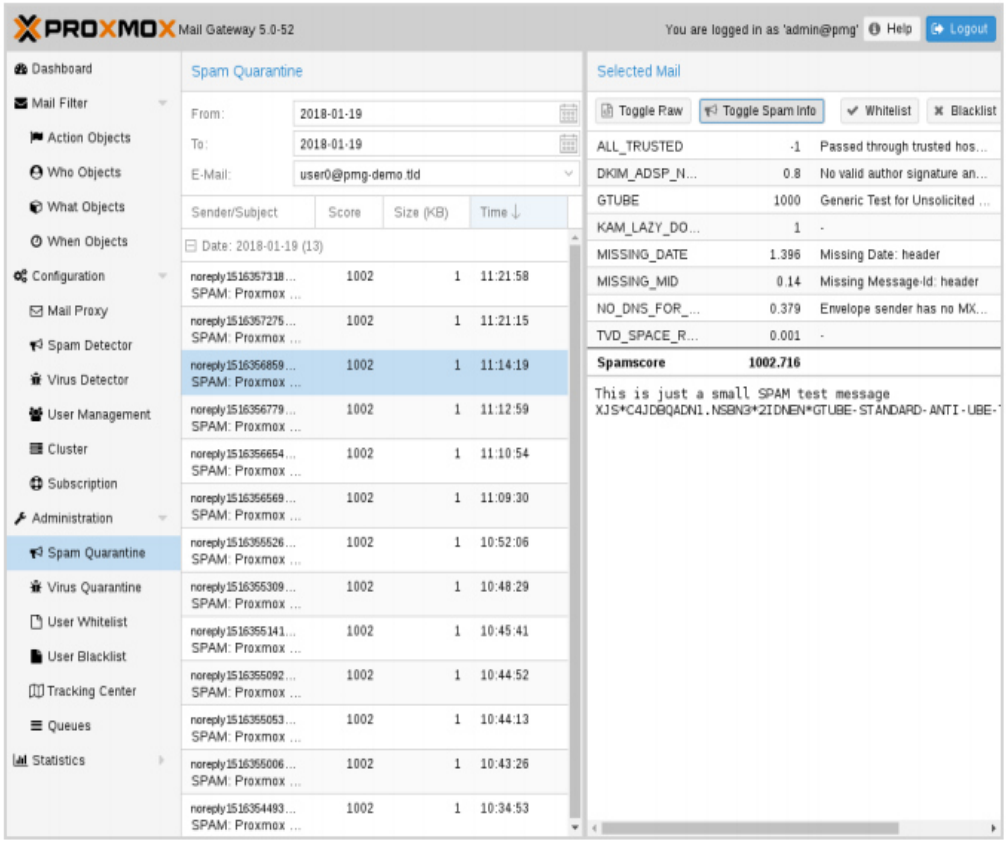
Сурет 3.36 – Сервердің жаңартуларын қадағалайтын бөлімше

3.37 суреттегі бетте қол жетімді жаңартулар көрсетілген және әкімші жаңартуды бастау үшін түймесін басу арқылы шығарамыз.



Сурет 3.37 – Жұмыс барысында жиналатын логтар

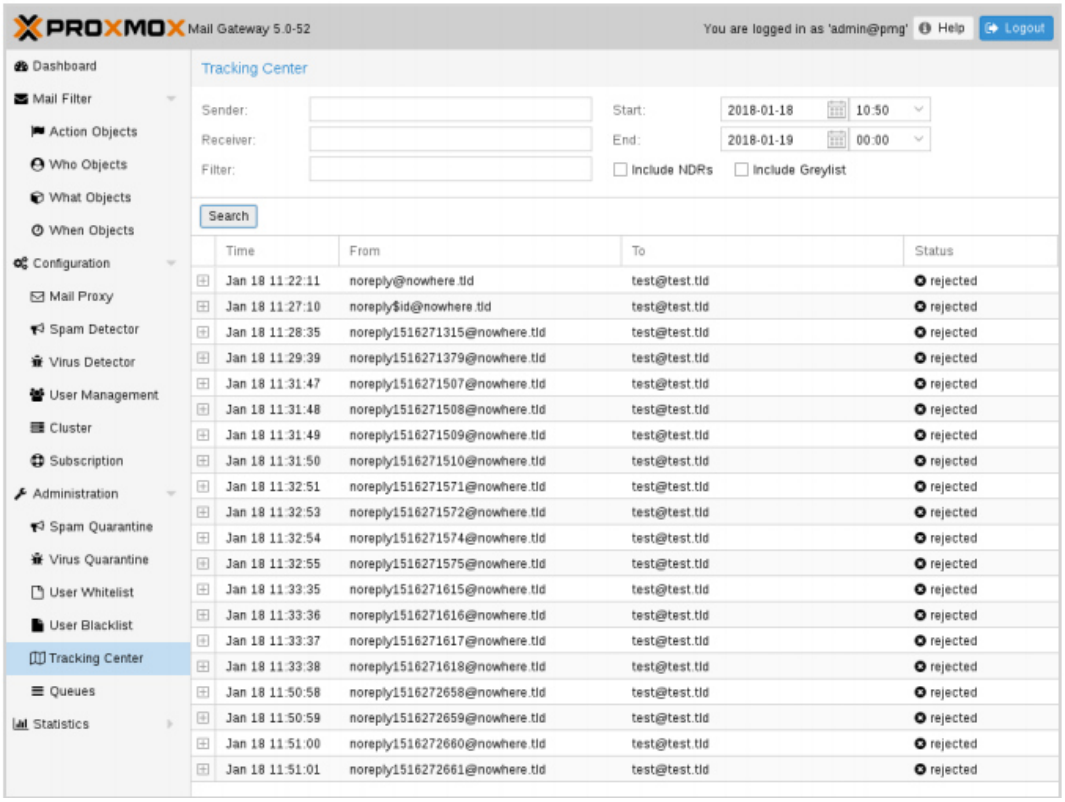
3.38 суретегі Syslog беті сізге нақты уақытта журналды жылдам көруге мүмкіндік береді.



Сурет 3.38 – Поштаны алдын ала қарау терезесі

3.39 суреттегі панель пошта карантинін тексеруге мүмкіндік береді. Электрондық хаттарды қауіпсіз көруге және бастапқы пайдаланушыға жеткізуге болады.

Веб-интерфейсте электрондық поштаны алдын ала қарау өте қауіпсіз, өйткені зиянды код пайда болады, сол үшін 3.39 суреттегі превью парақшасы бар.



Сурет 3.39 – Ортақ пошталарды қадағалайтын бөлімше

Электрондық пошта өңдеу күрделі міндет болып табылады және бірнеше қызмет домендарын қамтиды. Әрбір домен ақпаратты жүйелік журнал қызметіне жазады. Мәселе серверлер көптеген хаттарды параллель талдайды, сондықтан әдетте белгілі бір поштаға сәйкес келетін барлық журналдарды табу өте қиын.

Біз жүйелік журналдың қол жетімді деректерін іздеу үшін жоғары оңтайландырылған C кодын пайдаланамыз. Бұл өте тез және қуатты, және күніне бірнеше миллион хаттарды өңдейтін сайттар үшін жұмыс істейді

Нәтижесі 3.2 кесте деректерді қамтитын алынған хаттардың тізімі болып табылады:

Кесте 3.2 – Іс әрекет маркері

Уақыт	Жүйелік журналдың бірінші табылған жазбасының уақытша белгісі.
Қайдан	Мекен-жайдан (жіберушіден) Конверт.
Кімге	Электрондық пошта алушының мекенжайы
Статус	Жеткізу мәртебесі.
Системдік логтар	Жүйелік журналдың тиісті жазбалары

Мәртебе өрісінде электрондық поштамен не болып жатқанын қосады. Proxmox пошталық шлюзі-бұл пошталық прокси, яғни прокси поштаны сырттан алады, оны өңдейді және алушыға нәтижені жібереді.

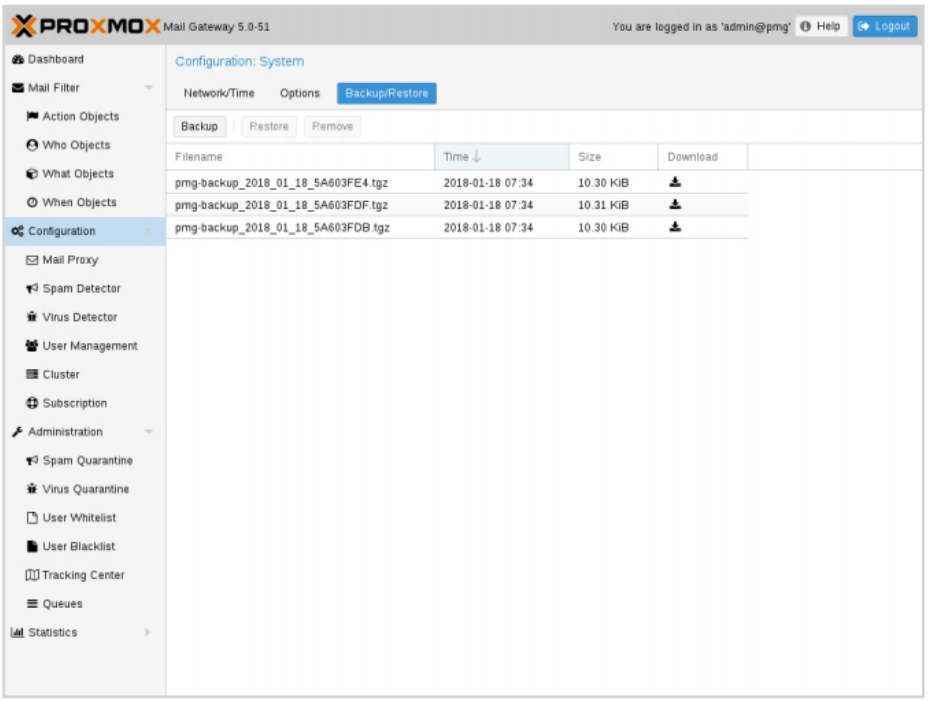
Бірінші кезең-пошта алу. Прокси-сервер поштаны бұрын қабылдамауы мүмкін немесе оның орнына поштаны қабылдап, оны сүзгіге береді. Сүзу ережелері поштаны бұғаттай немесе қабылдай алады.

Екінші кезеңде қабылданған хаттар алушыға жеткізілуі тиіс және бұл әрекет сәтсіз немесе сәтті аяқталуы мүмкін. Мәртебе бірінші және екінші кезеңдердің нәтижесін біріктіреді:

Кесте 3.3. Хат келу\кету мәртебелері

Статус	Фазасы	Сипаттамасы
Rejected	1	Электрондық пошта қабылданбады (мысалы, жіберушінің IP мекенжайы IP-адрестердің қара тізімінде көрсетілген)
Greylisted	1	Электрондық пошта уақытша сұр листингпен қабылданбады
queued/deferred	1	Ішкі электрондық пошта кезекке тұрды
queued/bounced	1	Ішкі электрондық пошта кезекке қойылған, бірақ мақсат қабылданбаған пошта сервері
Quarantine	1	Электрондық пошта карантинге ауыстырылды
Blocked	1	Электрондық пошта сүзгілеу ережелерімен құлыпталған
accepted/deferred	2	Электрондық пошта қабылданды, әлі де жеткізуге тырысады
accepted/bounced	2	Электрондық пошта қабылданады, бірақ мақсатты пошта серверімен қабылданбайды

3.40 суреттегі сақтық көшірме каталогта сақталады /var/lib/pmg/backup/. Әдетте қашықтағы файлдық жүйені осы каталогқа орнату жақсы.



Сурет 3.40 – Сақтық көшірме бөлімшесі

4 Техникалық–экономикалық негіздеме

4.1 Пошта сервері қауіпсіздігінің құрылымын жобалаудың күрделілігін анықтау

Сонымен қатар, бұл серверді қорғау үшін барлық тапсырмаларды қарапайым кезеңдерге бөлу қажет. ПҚ талдау күрделілігін үлестіру моделі 4.1 кестеде көрсетілген.

Кесте 4.1 – Пошталық сервер қауіпсіздігін құрастыру

Жоба кезеңі	Жұмыс түрі	Еңбек сыйымдылығы, адам сағ.
Кезең 1	Пошта серверін қорғау жөніндегі алғашқы кеңес	24
Кезең 2	Жергілікті есептеу желісі трафигінің инфрақұрылымын талдау	15
Кезең 3	Пошта трафигі бойынша талдау	8
Кезең 4	Жергілікті есептеу желісі трафигінің инфрақұрылым жобасын әзірлеу	30
Кезең 5	Пошталық трафик желісінің жобасын әзірлеу	20
Кезең 6	Жабдықты таңдау	34
Кезең 7	Домен контроллері пошта пайдаланушылар үшін құрылымды жобалау	5
Кезең 8	Енгізу және іске асыру	80
Кезең 9	Тестілеу	48
Кезең 10	Атқарылған жұмыстың қорытындысын шығару	10
Жиыны: дипломдық жобаны орындаудың еңбек сыйымдылығы		274

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық өнімді іске асыру үшін 34 жұмыс күні қажет.

4.2 Пошта серверін қорғауды жобалау шығындарын есептеу

Пошта серверін қорғауды жобалаудың қажетті шығындарын анықтау қолда бар смета негізінде жүргізіледі, ол мынадай элементтерді қамтиды:

- материалдық шығындар;
- еңбекақы төлеу шығындары;
- әлеуметтік салық;
- негізгі қорлардың амортизациясы;
- өзге де шығындар.

Материалдық шығындар адам тұлғасының белгілері бойынша аутентификация құрылымын жобалау үшін қажетті материалдарға, энергияға және басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 4.2 кестеде берілген нысан бойынша жүргізіледі[9].

Кесте 4.2 – Материалдық ресурстарға арналған шығындар

Материалдың атауы	Марка	Бірлік өлшеу	Саны	Бағасы теңгемен бірлік	Сомасы теңгемен.
Бумага для офиса	SvetoCopy	Упаковка	1	1 500,00	1 500,00
Дәптер (96 листов)	Abdi	Дана	10	250,00	2500,00
Блокнот	Abdi	Дана	2	1000,00	2000,00
Қаламдар	Abdi	Дана	10	50,00	500,00
Итого:					6 500,00

Пошта серверін қорғауды жобалау үшін SuperChassis 731D-300B CSE-731D-300B сервері пайдаланылады, сервердің қуаты қойылған міндеттерді орындау үшін жеткілікті. Сервер үшін операциялық жүйені және бағдарламалық жасақтаманы орнату қажет.

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге:

$$З_м = \sum P_i * Ц_i, \quad (4.1)$$

онда P_i - материалдық ресурстың і түрінің шығысы, заттай бірліктер;

$Ц_i$ - материалдық ресурстың і түрінің бірлігі үшін баға, тг;

і - материалдық ресурстың түрі;

n - материалдық ресурстар түрлерінің саны.

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 4.3-кестеде келтірілген нысан бойынша жүргізіледі..

Кесте 4.3 – Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

Материалдың атауы	Марка	Бірлік өлшеу	Саны	Бағасы теңгемен бірлік	Сомасы теңгемен.
Сервер	SuperChassis 731D-300B CSE-731D-300E	Дана	1	64 169,00	64 169,00
Роутер	ZyXEL ZyWALL USG20	Дана	1	70 545,00	70 545,00
Операциялық жүйе	Microsoft Windows Server 2016 R2	Лицензия	1	25000,00	25000,00
Пошта сервері	MicrosoftExchange 2012	Лицензия	4	34 800,00	34 800,00
Итого:					194 514,00

$$З_м = 6\ 500 + 194\ 514{,}00 = 201\ 014{,}00 \text{ (тг)}$$

Адам белгілері бойынша аутентификация құрылымын жобалауды жүзеге асыру үшін 201 014,00 теңге сомаға материалдар қажет.

4.3 Электр энергиясына арналған шығындарды есептеу

Электр энергиясын тұтынбай-ақ, адамның пошта серверін қорғауды жобалау кезінде электр энергиясын тұтынбай-ақ, электр энергиясына жұмсалатын шығындарды есептеу мәні бар.

4.1-кестеге сәйкес пошта серверін қорғауды жобалау үшін шамамен 318 сағат қажет, енді 318 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет.

$$Э = З_{эл.қ.} + З_{қос.к.}, \quad (4.2)$$

Онда $З_{эл.қ.}$ – жабдықтың электр энергиясына арналған шығындары;

$З_{қос.к.}$ – қосымша қажеттіліктерге арналған электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$З_{эл.қ.} = \sum W * К_{исц} * S * T, \quad (4.3)$$

онда W – тұтынылатын қуат, Вт;

$К_{исц}$ – пайдалану коэффициенті ($К_{исц}$ = 0,7 - 0,9);

Т – время работы;

S – тариф (1кВт/ч = 23,85тг заңды тұлғаларға арналған тариф "АлматыЭнергоСбыт" ЖШС» 01.01.19).

Жұмсалған электр энергиясының құнын есептеу қорытындылары 4.4-кестеде берілген.

Кесте 4.4 – Электр энергиясына арналған шығындар

Аспаптардың атауы	Төлқұжат қуаты, кВт	Төлқұжат қуаты	Жабдықтың жұмыс уақыты, ч	ЭЭ бағасы тг/кВтч	Сомасы, тг.
Сервер	0,45	0,9	274	23,85	2646,63
Роутер	0,22	0,7	274	23,85	1006,37
Жарық	0,2	0,7	274	23,85	914,88
Итого:					4567,88

$$З_{эл.эн.обор.} = 4567{,}88(\text{тенге})$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$З_{доп.нужды} = 5\% * З_{эл.эн.обор.}, \quad (4.4)$$

Формулаға сәйкес қосымша қажеттіліктерге арналған шығындарды анықтаймыз (4.4):

$$З_{доп.нужды} = 0.05 * 4567{,}88 = 228{,}39 \text{ (тенге)}$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 228{,}39 + 4567{,}88 = 4796{,}27 \text{ (тенге)}$$

4.4 Еңбекақы төлеу шығындарын есептеу

Бұрын көрсетілгендей, пошта серверін қорғауды жобалау үшін үш қызметкер қажет:

- жоба жетекшісі-жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;

-желілік әкімші-желілік трафиктің қол жетімділігін және оның өзгермейтіндігін қамтамасыз ету.

- пошта әкімшісі-белгілі бір пайдалану уақытында пошта жұмысына жауапты адам. Әрі қарай есептерді анықтау және қателерді әдейі іздеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{тр} = \sum ЧС_i * T_i \quad (4.5)$$

онда $ЧС_i$ - і-ші қызметкердің сағаттық мөлшерлеме, тг;

T_i - модельді әзірлеудің еңбек сыйымдылығы, чел.×ч; і - қызметкердің санаты;

n - ПҚ әзірлеумен айналысатын қызметкерлердің саны.

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық ставкасын және жалпы жалақы көлемін белгілеу мағынасы бар.

Часовую ставку қызметкерінің есептеуге болады мынадай формула бойынша:

$$ЧС_i = \frac{ЗП_i}{ФРВ_i} \quad (4.6)$$

онда $ЗП_i$ - і қызметкердің айлық жалақысы, тг;

$ФРВ_i$- і қызметкердің айлық жұмыс уақытының қоры, час.

Басшының айлық жалақысы 280 000 теңгеге тең және ИТ-менеджердің айлық жалақысы 250 000 теңгеге тең, ал Бета-тестілеушілер жалақыны 120 000 теңгеге алады. Есептейміз часовую ставку әрбір қызметкердің формулаға сәйкес (4.6):

$$ЧС_{руководитель} = \frac{230\,000}{22 * 8} = 1307 тг/ч$$

$$ЧС_{Почт.адм} = \frac{185\,000}{22 * 8} = 1051\ тг/ч$$

$$ЧС_{сет.админ} = \frac{200\,000}{22 * 8} = 1136\ тг/ч$$

Жоба жетекшісінің сағаттық мөлшерлемесі 1307 (тг/сағ) құрайды, әзірлеудің еңбек сыйымдылығы 100 сағатқа тең. Пошта әкімшісінің сағаттық ставкасы 1051 (тг/сағ) құрайды, жобалау және іске асырудың еңбек

сыйымдылығы 200 сағатқа тең. Желілік әкімшінің сағаттық ставкасы 1136 тең (тг/сағ). (4.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығындар сомасын есептеуге болады:

$$З_{тр} = 1307 * 100 + 1051 * 274 + 1136 * 274 = 130\,700{,}00 + 287\,974{,}00 + 311\,264{,}00 = 729\,938{,}00(\text{тенге})$$

Еңбекақы төлеу бойынша шығындардың есебі (4.5) кестеде көрсетілген

Кесте 4.5. – Еңбекақы төлеуді есептеу

Қызметкердің санаты	Біліктілігі	Еңбек сыйымдылығы ПП, час.	сағаттық мөлшерлеме, тг/ч	Сомасы, тг.
Басшы	Жоба жетекшісі	100	1307	130 700,00
Пошта администраторы	Microsoft СВТ	274	1051	287 974,00
Желілік администраторы	Сертификация Cisco	274	1136	311 264,00
Итого:				729 938,00

4.5 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық кодексіне сәйкес әлеуметтік салық еңбекақы қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

$$С_{н} = (ФОТ - ПО) * 0{,}095 (4.7)$$

онда ПО - зейнетақы қорына аударымдар, олар ЕТҚ-ның 10% құрайды.

$$ПО = 729\,938{,}00 * 0{,}1 = 729\,93{,}00 \text{тенге}$$

$$С_{н} = (729\,938{,}00 - 729\,93{,}00) * 0{,}095 = 62\,409{,}775 \text{тенге}$$

Есептеу нәтижелері кестеде берілген (4,6):

Кесте 4.6 – Әлеуметтік салықты есептеу

Қызметкердің санаты	Адам саны	жалақы, тг	Пенсионные отчисления, тг	Әлеуметтік салық, тг
Басшы	1	130 700,00	13 070,00	12 416,50
Пошта администраторы	1	287 974,00	28 797,00	27 357
Желілік администраторы	1	311 264,00	311 26,00	29 570,00
Итого:				69 344,11

4.6 Негізгі қорлардың амортизациясы және өзге де шығындар

Амортизация нормалары ҚҚ анықтау қажет салық кодексіне сәйкес. ОФ амортизациясын келесі формула бойынша анықтауға болады:

$$A_{\text{г}} = \frac{\text{С}_{\text{об}} * \text{Н}_{\text{а}}}{100} \quad (4.8)$$

онда, $\text{С}_{\text{об}}$ – жабдықтың құны;

$\text{Н}_{\text{а}}$ – амортизация нормасы (амортизация нормасы = 25);

(4.8) Формула сервер үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{\text{г}} = \frac{194\,514 * 25}{100} = 48\,628{,}50 \text{ тенге}$$

Енді жобалау кезеңінде амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{148\,628 * 34}{365} = 13\,844{,}80 \text{ тенге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеунәтижелерікестедекелтірілген (4.7).

Адам тұлғасының белгілері бойынша аутентификация құрылымын жобалауға арналған шығыстар сметасы.

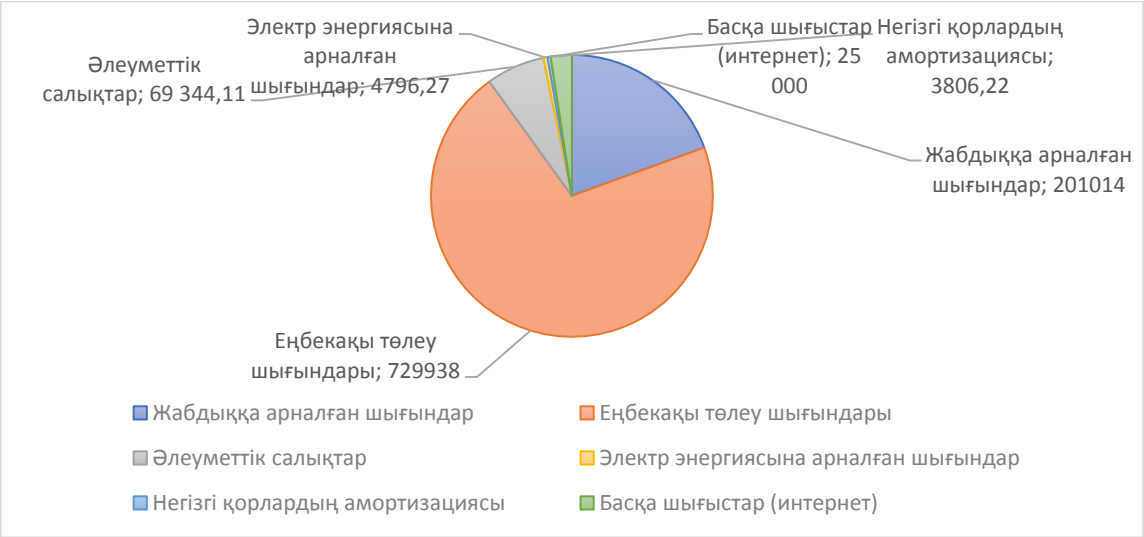
Барлық ұсынылған есептеулер негізінде пошта серверін қорғау құрылымын жобалауға арналған шығындар сметасын (4.7) кестеде келтірілген нысанға сәйкес ресімдеу қажет. 4.1-суретте жұмыс шығындарының диаграммасы көрсетілген.

Кесте 4.7 – Амортизация ОФ

Жабдық және БҚ атауы	Жабдықтармен БҚ құны, тг	Жылдық амортизация нормасы, %	Жыл ішіндегі амортизация сомасы, тг	Әзірлеу кезіндегі амортизация сомасы, тг
Сервер	64 169,00	25	16 042,25	1 494,34
Межсетевой экран (Роутер)	70 545,00	20	14 109,00	1 314,26
Операциялық жүйе	25000,00	15	3 750	349,30
Пошта сервері	34 800,00	20	6960,00	648,32
			Итого:	3 806,22

Кесте 4.8 – ПҚ әзірлеуге арналған шығындар сметасы

Шығындар баптары	Сомасы, тг
Жабдыққа арналған шығындар	201 014,00
Еңбекақы төлеу шығындары	729 938,00
Әлеуметтік салықтар	69 344,11
Электр энергиясына арналған шығындар	4796,27
Негізгі қорлардың амортизациясы	3806,22
Басқа шығыстар (интернет)	25 000,00
Итого по смете:	1 027 170 0,32



Сурет4.1 – Шығын диаграмма сы

4.7 Жобалаудың ықтимал бағасын анықтау

Бағдарламалық қамтамасыз етудің құны әзірленген өнімнің сапасы, оны әзірлеу мерзімі және өнімнің өнімділігі негізінде анықталады. Бағдарламалық қамтамасыз ету үшін Ц_Д құнын мына формула бойынша есептеуге болады:

$$Ц_Д = З_{нир}\left(1 + \frac{P}{100}\right), \quad (4.9)$$

онда$З_{нир}$ - бағдарламалық қамтамасыз етуді әзірлеуге арналған шығындар, тг;

Р – БҚ рентабельділігінің орташа деңгейі, (%). Бұл параметр 25% тең.

$$Ц_Д = 1\,027\,170{,}21\left(1 + \frac{25}{100}\right) = 1\,027\,170{,}21 + 256\,792{,}55$$
$$= 1\,283\,962{,}76 \text{ тенге}$$

Бұдан әрі ҚҚС есебімен сату құнын анықтау қажет, ҚҚС ставкасы ҚР заңнамасымен белгіленеді. 2019 жылға ҚҚС ставкасы 12% құрайды. Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады мынадай формула бойынша:

$$Ц_р = Ц_д + Ц_д * НДС, \quad (4.10)$$

$$Ц_р = 1\,027\,170{,}216 + 1\,283\,962{,}76 * 0{,}12 = 1\,181\,245{,}74 \text{ тенге}$$

Бұл бағаны1 181 245,80 тенге дейін дөңгелектеуге болады

5 Өміртіршілік қауіпсіздігі

5.1 Еңбек жағдайларын талдау

Бұл дипломдық жобада мен биометрияға негізделген бағдарламалардың тиімділігін зерттедім, атап айтқанда, бетті тану, сондай-ақ сол қағидатқа негізделген бағдарламаны әзірлеуді байқадым.

Дипломдық жобаның бұл бөлімі келесі мәселелерді қарастыруға арналған [10]:

– бағдарламашының жұмыс орнын ұйымдастыру;

– программист еңбегінің оңтайлы жағдайларын анықтау;

– программистің ақпараттық жүктемесін есептеу.

Жұмыс орнын дұрыс ұйымдастыра отырып, қызметкердің еңбек өнімділігін 8-ден 20 пайызға дейін көтеруге болады.

СанПиН-ге сәйкес 2.2.2/2.4.1340-03 жұмыс орнының құрылымы және оның барлық элементтерінің өзара орналасуы антропометриялық, физикалық және психологиялық талаптарға сәйкес болуы тиіс. Жұмыс өте маңызды орын алады. Ал нақты айтқанда, бағдарламашы жұмыс орнын ұйымдастыра отырып, келесі негізгі шарттарды сақтау қажет:

– жұмыс орнының құрамына кіретін жабдықтарды оңтайлы орналастыру;

– барлық қажетті қозғалыстар мен қозғалыстарды жүзеге асыруға мүмкіндік беретін жеткілікті жұмыс кеңістігі;

– қойылған міндеттерді орындау кезінде қажетті табиғи және жасанды жарықтандыру;

– акустикалық шудың деңгейі рұқсат етілген мәннен аспауы тиіс.

Жазбаша үстел және кресло - бағдарламашы жұмыс істейтін орынның басты элементтері. Отырудың жағдайы негізгі жұмыс жағдайы болып табылады. Отырған жағдайда жұмыстарды орындауға арналған жұмыс орны санитарлық ережелер мен нормаларға сәйкес ұйымдастырылады. 2.2.2/2.4.1340-03 [10].

Жұмыс қалпы отырып негізгі болып табылады, өйткені қабілетті тудыруы ең аз қажу программиста. Жұмыс орнын ұтымды жоспарлау заттарды, еңбек құралдарын және құжаттаманы орналастырудың нақты тәртібі мен тұрақтылығын көздейді. Жұмысты орындау үшін талап етілетін нәрсе жұмыс кеңістігінің жеңіл қол жеткізу аймағында орналасқан.

Жұмыс орнының параметрлері антропометриялық сипаттамаларға сәйкес таңдалады. Осы деректерді есептерде пайдалану кезінде ең жоғары антропометриялық сипаттамалардан (М+2).

5.1 суретте: а – максималды қолжетімді аймақ, б - қол созылған кезде саусақтардың қол жетімділік аймағы, в - алақанның жеңіл қол жеткізу аймағы, г – жуан қолмен жұмыс істеуге арналған оңтайлы кеңістік, д - жіңішке қолмен жұмыс істеуге арналған оңтайлы кеңістік.

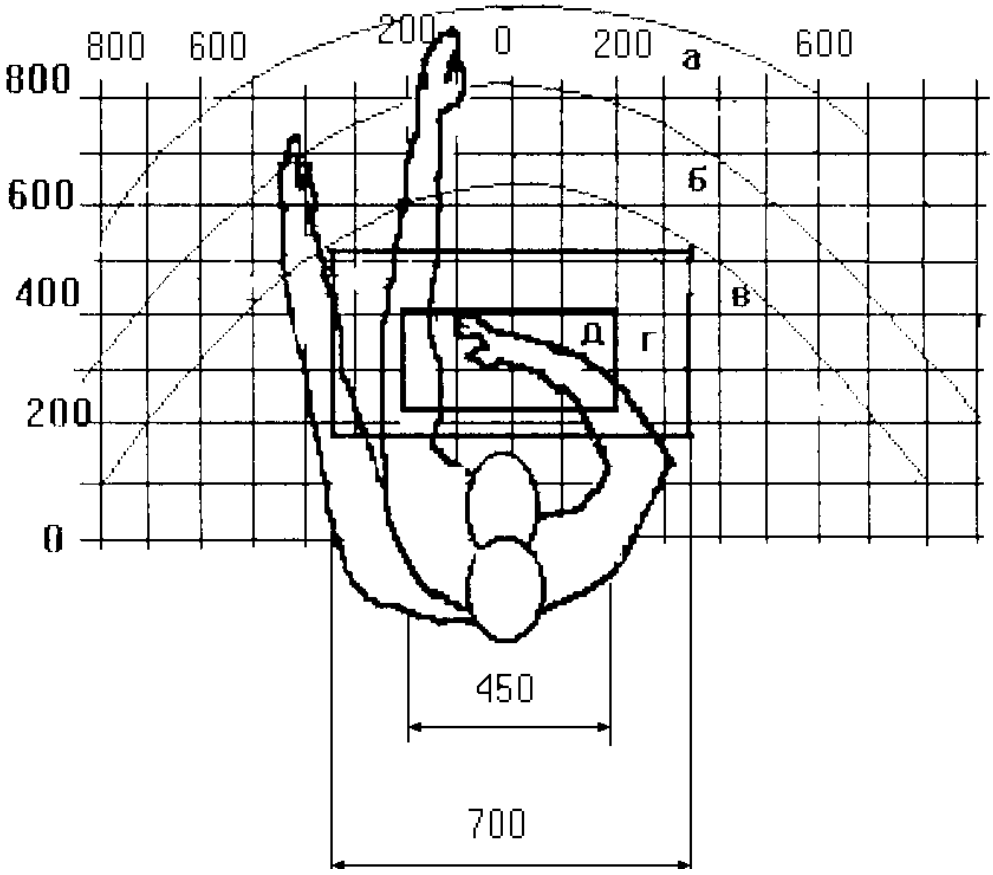
Жұмыс үстелін жобалау кезінде келесілерді қарастырған жөн:

– үстелдің биіктігі таңдалуы тиіс, бұл қажет болған жағдайда қолды ұстайтын ыңғайлы жағдайда, отыруға ыңғайлылықты қамтамасыз етеді;

– үстелдің төменгі бөлігін жобалау кезінде, бағдарламашының аяғын баспай-ақ, жайлы отыруға мүмкіндігін ескеру;

– үстелдің үстіңгі жағы қызметкердің радиусында жылтырлығы мен көріністерінің пайда болуына жатпайтын маңызды;

– кесте құрылғысы жәшіктердің болуын ескеруі тиіс (құжаттарды сақтауға кем дегенде 3, тізімдер, кеңсе, жеке қолданыс заттар бар).



Сурет5.1 – Көлденең жазықтықтағы қол жетімділік аймағы

Программистіңжұмысорнының маңыздықұрамдасбөлігікреслоболыптабылады. ОлГОСТ 21.889-76 сәйкесорындаладыКреслолардыжобалаукезіндепрограммистіңкезкелгенжұмысжағдайындаоның позасыфизиологиялықдұрыснегізделгенболуыкерек, яғниденебөліктерініңорналасуыоңтайлыболуыкерек. Орындықтаадамденесініңжағдайынталдаудантуындайтынфизиологияталаптарынқанағаттандыруүшінжұмысорындығының конструкциясыкелесінегізгіталаптардықанағаттандыруытиіс:

– дене корпусының және оның аяқ-қолдарының бір-біріне қатысты еркін қозғалуына жол беру;

– программистің өсуіне сәйкес биіктіктің өзгеруіне жол беру (400 мм-ден 550 мм-ге дейінгі шектерде));

– аздап қисық беттің болуы,

– артқа жеңіл көлбеу болуы.

Жоғарыда айтылғандарды ескере отырып, бағдарламашы үстелінің параметрлерін келтіреміз:

– үстел биіктігі 710 мм;
– үстел ұзындығы 1300 мм;
– үстел ені 650 мм;
– үстел тереңдігі 400 мм.

Жазу беті:

– 40 мм тереңдікте;
– ені 600 мм.

Еңбекжағдайларынұйымдастыружәнежұмыстажұмыскеңістігіндұрысэстетикалықбезендіру. Еңбекті жеңілдету үшін де, еңбек тиімділігі мен өнімділігіне қолайлы әсер ететін оның тартымдылығын арттыру үшін де маңызды рөл атқарады. Үй-жайлар мен жағдайдың түсі жұмысқа ынталандыра отырып, көзбен қабылдау үшін қолайлы жағдайлар жасауға ықпал етуі тиіс. Елеулі жүйке кернеуін және аз шоғырлануын талап ететін рутинді ақыл - ой жұмысы жүзеге асырылатын қызметтік үй-жайларда түсі бейтарап тондар-суық жасыл немесе көгілдір түстердің пастельді реңктері болуы тиіс.

Қызметкердің ең жақсы еңбек жағдайларын ұйымдастыра отырып, жарықтандыруды, Шу мен микроклиматты қарастыру қажет.

5.2 Оператор отыратын бөлмесінің жарықтандыруын есептеу

Табиғи жарықтандыру әлсіз болғандықтан, жұмыс орнында жасанды жарықтандыруды пайдалану қажет. Бұл пунктте жасанды жарықтандыру есебі ұсынылады. Жұмыс орнында мұндай жарықтандыруды жасау қажет, ол жұмысшыға шаршамай және көру органдарын кернеусіз жұмыс істеуге мүмкіндік береді. Көру мүшелерінің шаршауы бірқатар себептерге байланысты:

– жарықтың жеткіліксіздігі;
– шамадан тыс жарықтандыру;
– жарықтың дұрыс емес бағыты.

Жұмыс орнының жарықтандырылуын есептеу жарық жүйесін таңдау, шамдардың қажетті санын, олардың түрін және орналасуын анықтау болып табылады. Барлық нюанстарды біле отырып, жасанды жарықтандыру көрсеткіштерін есептейміз.

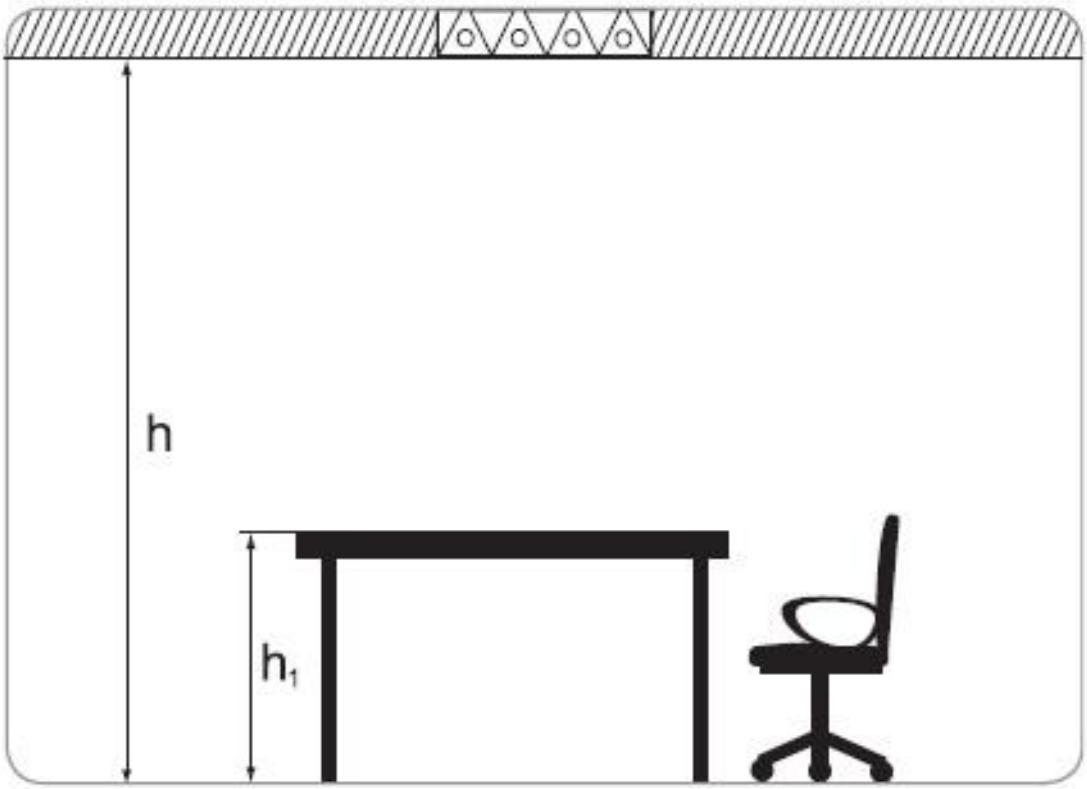
Жасанды жарықтандыру екі түрлі жарық көздері арқылы жүзеге асырылады: қыздыру шамдары және люминесцентті шам. Сонымен қатар, 4.2-суретте үй-жайдың биіктігі мен есептік биіктіктің арақатынасы көрсетіледі [11].

Бөлменің ауданын анықтау:

$$S = a \times b, \qquad (5.1)$$

мұндағы a – ұзындық;
b –ені.
Бөлме индексін анықтау:

$$I = \frac{S}{(h-h_1)\times(a+b)} \quad (5.2)$$



Сурет5.2 – Бөлме биіктігі мен есептік биіктіктің арақатынасы

Шамдардың қажетті санын анықтау:

$$N = \frac{100\times E\times S\times K_з}{U\times n\times Ф_л}, \quad (5.3)$$

мұндағыE — көлденең жазықтықтың қажетті жарықтануы, лк;
S — үй-жай ауданы, м^2;
Кз — қор коэффициенті (Кз =1,25);
U — қондырғыны пайдалану коэффициенті;
Фл — бір шамның жарық ағыны, лм;
n — шамдағы лампалар саны.
Осылайша:
Кеңсе: "Каспий" аспалы төбелер, ақшыл жасыл тұсқағаздар, сұр кілем.
Бастапқы деректер:
Үй-жай: a = 5 м, b = 4 м, h =3 м
Шам: TLC418
Лампалар: люминесцентті 18 Вт, бір шамда 4 лампа Фл = 1150 лм

Жарықтандыру нормалары: Е = 500 лк еденнен 0,8 м деңгейінде
Қор коэффициенті: Кз = 1,25
Шағылысу коэффициенті: төбе — 50, қабырға — 30, еден — 10
Үй-жай ауданын анықтаймыз:

$$S = 5 \times 4 = 20 \text{ м}^2$$

Үй-жай индексін анықтаймыз:

$$I = \frac{20}{(3 - 0{,}8) \times (5 + 4)} = 1$$

5.2-кестеде берілген бөлменің индексі мен шағылысу коэффициенттерінің мәндеріне сүйене отырып, пайдалану коэффициентін анықтаймыз: U=48

Кесте5.2 – Пайдалану коэффициенті

TLC418								
Төбе	80	80	80	70	50	50	30	0
Қабырғалар	80	50	30	50	50	30	30	0
Еден	30	30	10	20	10	10	10	0
i=0,6	59	42	35	41	39	35	35	31
i=0,8	66	50	43	48	46	42	41	37
i=1	71	56	48	54	51	47	46	42
i=1,25	77	63	54	60	56	53	52	49

Шамдардың қажетті санын анықтаймыз:

$$N = \frac{100 \times 500 \times 42 \times 1{,}25}{48 \times 4 \times 1150} = 11{,}9$$
$$N = 11{,}9 \sim 12 \text{ шам}$$

5.3 Электромагниттік сәулелердің адамға әсері

Электромагниттік сәулелердің адам ағзасына неге зиянды екенін анықтайық [12].

Адам ағзасы да электрлік импульстерді шығарады. Олардың көмегімен ми мен жұлынға жүйке үштары арқылы сигналдар келіп түседі, қаңқа бұлшықеті мен жүрек бұлшықеттері азаяды. Жүйке үштары арқылы секундына мыңдаған сигналдар беріледі, сондықтан компьютерден қандай зиян келетінін оңай түсінуге болады, сәулелер электрлік импульс жіберудің қиын жүйесіне әсер етіп, олардың өзара байланысына бөгет келтіруі мүмкін. Оның әсері бір сәтте сезілмейді,ол ағзада жинақталып, мүшелер мен жүйелердің жұмысын біртіндеп нашарлатады.

Екі маңызды жүйе ең осал болып табылады:

– жүйке жүйесі;

- жүрек – қан тамырлар жүйесі.

Бұның әсерінен ми сигналдары патологиялық түрде өзгеруі мүмкін. Бұл мидың және жүрек-тамыр жүйесі органдарының бұзылуына себеп болады. Жүрек-қантамыр жүйесінің қалыпты жұмыс істеуі импульстердің когеренттігіне және беріктігіне байланысты. Үйдегі бір немесе одан да көп құрылғылар жүрек жұмысын елеулі бұзылуға алып келмейді, бірақ үнемі сәулелену аритмия мен жүрек-тамыр қабілетінің бұзылуына әкелуі мүмкін. Ұзақ уақыт бойы әсер етуі бас ауруы, мигреньдер, иммунитеттің төмендеуі, депрессия, гормоналды теңгерімсіздік және ұйқының бұзылуына әкелуі мүмкін. Компьютерде көп жұмыс істеу Альцгеймер ауруы, Паркинсон ауруы, қатерлі ісік ауруы және ұрпақты болу жүйесінің бұзылу қаупін арттырады. Сонымен қатар миокард және перикард ауруларына, ағзаның жалпы гормональды фонының бұзылуына, су-тұз алмасуының нашарлауына, гомеостаздың бұзылуына алып келуі мүмкін.

Үй компьютері, ноутбук немесе смартфон зиянды сәуле көзі болып табылады. Компьютерден қанша сәуле алатынымыз түрлі факторларға байланысты: құралдың түрі, пайдалану уақыты, орналасуы.

Кондиционер, егер жұмысшы біреудің бөлмесіне ие болса, онда қызметкердің жақсы микроклиматының бір жылын ұстап тұру керек еді, ол жұмыс уақытының барлық ауыртпалығы кезінде жұмыс үшін қажетті бөлмені оңтайлы күйде орналастырады. Үш адам бөлмені шаңнан шығаруды қажет етеді екі зиянды заттарды білдіретін басқа файл. Шабуылдарды орындау үшін бұл аз мөлшерде, үшеуі өте таза, біреуі таза бөлмеде жүргізіледі. Мұның бәрі, қоспағанда, ластаушы ауа арқылы бөлме шабуылының ауырсынуын болдырмауға мүмкіндік береді. Жабдықта болса да, бұл функциялар әуе файлын бөлу туралы ереже бойынша жекелендірілген болса да назарға алынады. Үш қызметкердің бөлмесінде жұмыс істейтін ең төменгі ауа температурасы кемінде 18 ° С кем емес

Оңтайлы жағдайлардың кодтарын қалыптастыру үшін бірқатар жұмысшылардың еңбек нормалары осы өндіріс микроклиматының барлық

нормалары ретінде анықталады. Дербес компьютердің шабуыл шотымен жұмыс жасағанда, SanPin 2.2.2 / 2.4.1340-03:

Жоғарыда суық мезгілде:

– 22-24 ° С температура файлын қалыпқа келтірді;

– рұқсат етілген ядролар - 18-26 ° С;

– ауаның салыстырмалы ылғалдылығы 40-60%;

– рұқсат етілген желі 75%.

Жылы кезеңде:

– температура 23-25 ° С-ге дейін қалыпты;

– рұқсат етілген дос 20-30 ° С;

– ауаның салыстырмалы ылғалдылығы 40-60%;

– қабырғалардың рұқсат етілген ылғалдылығы 55% құрайды.

Олардың кэшті орналасуы қарастырылған (5.1 суретте)

сипаттамалары:

– екі қабатты ғимараттың бірінші қабатында орналасқан;

– бір қызметкердің көлемі бір бөлме: ядро ұзындығы 4 м, ені 3 м, биіктігі 3 м;

– жасанды жарықтандыру - шамдар: әрқайсысында 2 шам

Әрқайсысының 2 люминесцентті лампасы (PVLM - 1 × 40);

– визуалды жағдайларға ауыр жұмыстардың ауырлығы жоғары IV санатына жатқызу, ең кішкентай нысан нысанды 1-ден 5 мм-ге дейін бөлетіндіктен;

– жұмыс орындарының саны.

2) Электромагниттік сәулеленуден қорғау тәсілдері

Электромагниттік сәулеленудің жағымсыз әсерінен қорғаудың ең тиімді тәсілдерінің бірі арнайы құралдарды қолдану болып табылады, ол осы сәулеленуді бейтараптандыруға және оның адам ағзасына теріс әсерін барынша азайтуға мүмкіндік береді. Бұл құралдардың жұмыс істеу принципі адам ағзасына жағымсыз электромагниттік сәулеленудің жағымсыз әсерін төмендетуге ықпал ететін қарсы ЭДС-ға негізделген.

Электромагнитті сәулеленудің әсер ету аймағында болу уақытын барынша қысқарту ағзаны электромагнитті сәулеленудің жағымсыз әсерінен қорғаудың ең тиімді тәсілдерінің бірі болып табылады. Бұл мәселе электрмагниттік сәулелену деңгейі ең жоғары электр энергетикалық кәсіпорындардың қызметкерлері үшін ерекше өзекті.

Мысалы, жоғары вольтты тарату қосалқы станциясына қызмет көрсететін персонал. Тарату құрылғыларында, ашық және жабық типті электромагниттік сәулелену деңгейі өте үлкен. 110кВ және одан жоғары электр қондырғыларында электромагниттік сәулелену деңгейі адам ағзасына теріс әсер етуі өте күшті болып табылады.

Алғашқы белгілер бірден пайда болады: бас ауруы, әлсіздік, тітіркену, тежелу. Мұндай жағдайларда адамның арнайы қорғаныш жинақтарын (экрандаушы құрылғыларды) пайдаланбай электромагниттік сәулеленудің әрекет ету аймағында болуына жол берілмейді.

Қызмет көрсететін персонал жоғары вольтты жабдықтан алыста болған кезде, мысалы, жалпы станциялы басқару пунктінде электромагниттік сәулелену деңгейі әлдеқайда аз, бірақ оның мәні рұқсат етілген мәндерден жүздеген есе асып түседі. Бұл бөлмеде көптеген электромагниттік сәулелену көздері бар: компьютерлік техника, қорғаныс құрылғылары және жабдықтың автоматикасы, төменвольтті тарату қалқандары және т. б.

Мұндай жағдайда, мүмкін болған жағдайда үзіліс жасап, үй-жайдан шығып, сол арқылы электромагниттік сәулелену аймағында болу уақытын қысқартқан жөн. Сондай-ақ, жоғарыда аталған құрылғыларды адам ағзасына электромагниттік сәулеленудің теріс әсерін азайтуға мүмкіндік беретін пайдалану артық болмайды.

5.4 Микроклимат параметрлері

Микроклиматтың мәндері кең шекараларда өзгерістерге ұшырайды. Сонымен қатар, адам ағзасының қоршаған ортаға жылудың жоғалуын бақылау қабілеті, тербеттеу функциясы арқылы дене температурасының тұрақтылығын сақтау болып табылады.

Микроклиматты реттеудің маңызды принципі-адам денесінің қоршаған ортамен жылу алмасуы үшін қолайлы жағдайларды ұйымдастыру. СН-245/71 санитарлық нормаларында оңтайлы жағдай жасайтын микроклимат параметрлерінің мәндері анықталған. Жыл уақытына, орындалатын жұмыстың сипатына және жұмыс үй-жайларының сипатына сәйкес (Елеулі немесе елеулі емес жылу бөлу) осы нормалар анықталады. 4.2-кестеде 20 ккал/м3 дейін артық жылу бөлетін өндірістік үй-жайлар үшін микроклимат параметрлерінің қолайлы және рұқсат етілген мәндері көрсетілген[12]:

Бүгінгі күні оңтайлы жағдайларды жасау үшін ұйымдастыру әдістері ғана емес, техникалық құралдар да қолданылады. Ұйымдастыру жұмыстарына жыл және тәулік уақытына сәйкес жұмыстарды жүргізуді ұйымдастыру, сондай-ақ еңбек пен демалыстың дұрыс үйлесімін ұйымдастыру орынды деп жатқызуға болады. Осыны ескере отырып, мекеме аумағында су айдынымен (бассейндер, субұрқақтар) және орындықтармен демалу үшін көгалдандырылған аймақты құру ұсынылады. Техникалық құралдарға желдету, ауаны баптау, жылыту жүйесі жатады.

Кесте 5.3 – Микроклимат параметрлерінің мәні

Жыл уақыты	Аймақ	Ауа Температурасы, ^{0} С	Салыстырмалы Ылғалдылық, %	Ауа қозғалысының жылдамдығы, м/с
Суық Кезең	Оңтайлы	18 - 21	60 - 40	< 0.2
Өтпелі Кезең	Рұқсат етілген	17 - 21	<75	< 0.3
Жылдың жылы кезеңі (t > 10^0 С)	Оңтайлы	20 - 25	60 - 40	< 0.3
	Рұқсат етілген	<28 ең ыстық айдың 13 сағатында.	<75	< 0.5

Қорытынды

Электрондық пошта Интернет желісінің ең танымал сервистерінің бірі бола отырып, ақпараттық қауіпсіздік тұрғысынан бірқатар қатерлерге ұшырайды. Сондықтан оны пайдаланудан экономикалық пайда алумен қатар, ұйымдар мен пайдаланушылар электрондық пошта сервисі арқылы зиянкестер келтірген зияннан зардап шегеді. Осыған байланысты криптографиялық әдістер, конент-талдау әдістері және ұйымдастыру шаралары негізінде осы сервистің қауіпсіздігі мәселелерін кешенді шешу қажет.

Жұмыстың негізгі нәтижелері:

– электрондық пошта жұмысының принциптері мен технологиялары, сондай-ақ оны кәсіпорын желілерінде пайдалану ерекшеліктері анықталды;

– электрондық хат алмасу мен электрондық пошта сервистеріне ықтимал қауіп-қатерлер және осы қауіптерден қорғау әдістері талданды;

– ақпаратты қорғау және электрондық хат алмасу саласындағы нормативтік-құқықтық база талданды;

– электрондық поштаны қорғаудың бағдарламалық құралдарының тиімділігін бағалау критерийлері анықталды;

– электрондық хат алмасуды қорғаудың заманауи бағдарламалық құралдарының нарығы талданды;

– кәсіпорында электрондық хат алмасу мен электрондық пошта сервистерін қорғау үшін оңтайлы шешімдер ұсынылды және негізделген , электрондық поштаны қорғау бойынша практикалық ұсыныстар әзірленді.

Әдебиеттер тізімі

1 Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. Москва: Горячая линия – Телеком, 2007.
2 Горбатов В.С., Полянская О.Ю. Основы технологии PKI. Москва: Горячая линия – Телеком, 2004.
3 Соколов Дмитрий, Подпись для электронного документа, Компания «Актив»,
4 Таранов А., Слепов О. Безопасность систем электронной почты.
5 Семенов Ю.А. Образовательный сервер "Телекоммуникационные технологии"
6 Блам Р. Администрирование почтовых серверов sendmail.
7 Информационная система по нормативным документам NormaCS
8 Кузьменкова О., Анализ рынка программных средств защиты компьютерных систем. Москва: Экстразащита, 2003.
9 Куатова Д.Я. Кәсіпорын экономикасы. –Алматы: «Экономика», 2011.
10 Байзаков А.А., Бегимбетова А.С., Дюсебаев М.К., Санатова Т.С. Еңбекті қорғау. Зертханалық жұмыстарды орындауға арналған әдістемелік нұсқаулар (күндізгі-сырттай оқу бөлімінің барлық мамандықтарының студенттері үшін). – Алматы: АИЭС, 2004.
11 СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы. М., 2003.
12 ГОСТ 21889-76. Система "Человек-машина". Кресло человека-оператора. Общие эргономические требования. М., 1976.