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

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі: с.ғ.к., доцент Бердібаев Р. Ш.
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____20____ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: Бұлттық сервистер қауіпсіздігіне мониторинг жасау және зерттеу_____

Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»

Орындаған: Жұмаханов Мадияр Бақытжанұлы_____ Тобы СИБк-16-1
(аты-жөні)

Ғылыми жетекші: т.ғ.к, доцент Шайкулова Актоты Алиевна_____
(ученая степень, звание, Ф.И.О.)

Мамандығы бойынша:
аға оқытушы Дмитриева Маргарита Валерьевна_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____20____ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
доцент Жандаулетова Фарида Рустембековна_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____20____ж.
(қолы)

Мөлшер бақылаушы: аға оқытушы Альмуратова Камшат Бимуратовна_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____20____ж.
(қолы)

Пікір беруші: РМК аға ғылыми қызметкері, PhD Шаяхметова Асем Серикбаевна
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____20____ж.
(қолы)

Алматы 2020

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

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент:Жұмаханов Мадияр Бақытжанұлы _____
(аты-жөні)

Жобаның тақырыбы: Бұлттық сервистер қауіпсіздігіне мониторинг жасау және зерттеу _____

2019 ж. «11» қараша №56 университет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «1» маусым 2020 ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): NIST стандарты бойынша бұлтты сервис бөліктеріне жекелей талдау және Отандық нарықта сұранысқа ие сервис түрін анықтау. Жиналған деректер негізінде IaaS сервистік модельінің компоненттеріне зерттеу. Сонымен қатар, бұлтты сервистерге төнетін қауіп түрлеріне мониторниг жасалу қажет және дайын қорғану амалдары ұсынылады. Осыған негізделе отырып шағын ұйымдарға арнлаған жеке бұлт құрылады.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:

1. Бұлттық сервистер сипаттамасы.
2. IaaS сервистік моделі.
3. Бұлттар қауіпсіздігне мониторинг.
4. Алғашқы өрт сөндіру құралдары және жерге тұйықтау есебі қажеттілігін есептеу.
5. Ақпараттық қауіпсіздік тәуекелдерін екі параметр бойынша бағалау.

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:

1.1 кесте. Бұлтты қызмет үлгілерін салыстыру

сурет 2.2 – Бұлтты жүйенің есептеу инфрақұрылымы

сурет 2.4 – Виртуальді және физикалық интерфейстермен vSwitch жалпы пайдалану сызбасы

2.1 кесте. Инфрақұрылымды басқару жүйелерінің мүмкіндіктерін салыстыру

2.2 – кесте. Отандық провайдерлердің қызмет түрлерін салыстыру.

сурет 3.13 – Қортынды шабуылдар үлесі

5.4 кесте – Тәуекелдерді бағалаудың қорытынды кестесі

Негізгі ұсынылатын әдебиеттер: 1. Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Software & Systems Программные продукты и системы // Облачные технологии: основные модели, приложения, концепции и тенденци и развития.

2. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing.Облачные вычисления.

3. Богомолов И. В., Алексиянц А. В., Борисенко О. Д. и др. (2016) Проблемы масштабируемости облачных сред и поиск причин деградации центрального сервиса идентификации Openstack Keystone.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
Негізгі бөлім	Шайкулова А.А.	03.03.2020ж	
Ө.Т.Қ.Н.	Жандаулетова Ф. Р.	13.04.2020ж	
А.Қ.Т.Е.	Дмитриева М. В.	20.04.2020ж	
Есептеу техникасы	Шайкулова А.А.	12.04.2020ж	
Нормабақылаушы	Альмуратова К.Б.	02.06.2020ж	

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
Бұлттық сервистер сипаттамасы	17.02.2020 – 20.02.2020	
Даму бағыты	21.02.2020 – 28.02.2020	
IaaS сервистік моделі	01.03.2020 – 08.03.2020	
IaaS сервитік моделін басқаруға арнлаған платформаларды салыстыру.	09.03.2020 - 18.03.2020	
Қазақстандық провайдерлер қызметтерінің салыстырмалы сипаттамасы	19.03.2020 – 27.03.2020	
Бұлттар қауіпсіздігне мониторинг.	28.03.2020 - 07.04.2020	
Жеке бұлт құру	08.04.2020 - 18.04.2020	
Өмір-тіршілік қауіпсіздігі бөлімі	19.04.2020 - 30.04.2020	
Ақпараттық қауіпсіздік тәуекелдері	01.05.2020 - 09.05.2020	

Тапсырманың берілген уақыты «12» қаңтар 2020ж.

Кафедра меңгерушісі _____ (Бердібаев Р. Ш.)
(қолы)

Жобаның
ғылыми жетекшісі _____ (Шайкулова А. А.)
(қолы)

Орындалатын тапсырманы
қабылдаған студент _____ (Жұмаханов М. Б.)
(қолы)

Аңдатпа

Дипломдық жобада бұлттық сервистер қауіпсіздігіне мониторинг және зерттеу жүргізілді. бұлтты сервистерге төнетін қауіп түрлері және қорғану амалдары көрсетілген. Осыған негізделе отырып, қауіпсіз жеке бұлт құрылды.

Жұмыс барысында OwnCloud, Apache, SQLlite, NoMachine бағдарламалары мен қауіпсіздік SSL/TLS сертификаты қолданылды.

Бұл диплом жобада еңбекті қорғау жөніндегі іс-шаралар және тәуекелдерді есептеу бөлім қарастырылады. Өміртіршілік қауіпсіздігі бөлімінде алғашқы өрт сөндіру құралдары және жерге тұйықтау есебі қажеттілігіне есеп жүргізілді, ал тәуекелдер бөлімінде активтерге төнетін қауіптерге байланысты есептеулер жүргізілді.

Аннотация

В дипломном проекте проведен мониторинг и исследование безопасности облачных сервисов. Также рассмотрены все аспекты безопасности облако и предложены меры по обеспечению безопасности. Основываясь на этом, создано безопасное личное облако.

В ходе работы были использованы программы OwnCloud, Apache, SQLlite, NoMachine и сертификат безопасности SSL/TLS.

Данный диплом в проекте рассматривается раздел по охране труда и расчет рисков. В части безопасности жизнедеятельности произведен расчет необходимости первичных средств пожаротушения и расчета заземления, а в части рисков проведены расчеты рисков, связанных с рисками возникновения активов.

Annotation

In the diploma project, the security of cloud services was monitored and studied. All aspects of cloud security are also considered and security measures are proposed. Based on this, a secure personal cloud is created.

During the work, the programs OwnCloud, Apache, SQLlite, NoMachine and the SSL/TLS security certificate were used.

This diploma in the project deals with the section on labor protection and risk calculation. In terms of life safety, the calculation of the need for primary fire extinguishing means and the calculation of grounding was made, and in terms of risks, the risks associated with the risks of assets were calculated.

Мазмұны

Кіріспе

Қазіргі заманда бұлтты технологиялардың өте қарқынды дамуда, бұл даму барысы жалпы технологиялардың ауқымына көп үлесін қосқанымен, кері жақтары да айтарлықтай бар. Мысалы, ақпарттық қауіпсіздік мәселесі өте өзекті болып табылады. Бұның бірден бір себебі көп ақпараттың бұлтты сервистерге ауысуы болып табылады, бұл құпия ақпарттардың ұрлануына және заңсыз түрде желі арқылы деректерге қол жеткізу сияқты құқық бұзушылықтардың өсуіне себеп болады. Сол себепті бұлтты сервистердің қауіпсіздік мәселесін талдау маңызды болып табылады.

Бұлтты есептеулер - серверлік ресурстар мен қуаттарды пайдаланушыға интернет - қызмет ретінде берілетін деректерді өңдеу және тарату технологиясы. Бұлттық есептеулер тұжырымдамасының мәні соңғы пайдаланушыларға интернет арқылы қызметтерге, есептеу ресурстарына және қосымшаларға (операциялық жүйелер мен инфрақұрылымды қоса алғанда) қашықтан қолдануға ммкүндік береді. Хостинг саласын дамыту бағдарламалық қамтамасыз ету мен сандық қызметтерде пайда болған қажеттілікке байланысты болды, оларды ішінен басқаруға болады, бірақ олар масштабтағы үнемдеу есебінен неғұрлым үнемді және тиімді болып табылады.

Алдағы 2-3 жылда бұлт кез келген кәсіпорын инфрақұрылымының ажырамас бөлігі болады. IDC зерттеу компаниясының болжамы бойынша 2022 жылға қарай ұйымдардың 70% бұлтты технологияларды пайдаланатын болады. Бұл ретте жаңа IT-инфрақұрылымның жартысынан астамы деректерді өңдеудің корпоративтік орталықтарында емес, сыртта орналасатын болады. Cloud-шешімдерді жаппай енгізілуде, дейді Gartner талдаушылары. Олардың бағалауы бойынша, биылғы жылы бұлтты сервистер нарығы $266,4 млрд.белгіге жетеді, бұл 2019 жылға қарағанда 17% - ға артық.

Қазақстанда бұлттық есептеулер бағытына қозғалмаған бірде-бір компания жоқ. Бұлтты ортаға тек орта немесе кіші бизнес емес, барлық мемлекеттік және ірі компанияларда көшуде. Бұған ел экономикасының даму қарқынын жеделдетуге және халықтың өмір сүру сапасын жақсартуға бағытталған "Цифрлық Қазақстан" мемлекеттік бағдарламасы да ықпал етеді. Электрондық денсаулық паспорты, Әлеуметтік ID, Smart City, "Сандық Жібек жолы", "Сот кабинеті" және "электрондық үкімет" – республикада енгізілгеннің аз ғана бөлігі. Айта кетсек, eGov.kz порталдының жұмыс уақытында eGov.kz азаматтарға 200 млн. жуық электрондық қызмет көрсетілді. 2020 жылы "цифрдағы" мемлекеттік қызметтердің үлесі 90% - ды құрайды, ал 2022 жылы қазақстандықтардың цифрлық сауаттылығының деңгейі 83% - ды құрайды деп болжануда.

1 Бұлттық сервистер сипаттамасы

Бұлтты есептеулер (ағылш. Cloud computing) – есептеу қуаты пайдаланушыға сервис ретінде берілетін деректерді өңдеу технологиясы. Пайдаланушы тек дербес деректерге қол жеткізе алады және жүйе негізінде жатқан бағдарламалық және аппараттық инфрақұрылымды басқара алмайды. "Бұлт" термині компьютерлік желілердің диаграммаларында интернет желісінің суретіне негізделген метафор ретінде немесе арнайы бағдарламалық деңгейде жасырын күрделі инфрақұрылым түрінде пайдаланылады.

Cloud computing негізінде бірнеше жолы бар. Біріншісі – интернет арқылы сервистердің қолжетімділігі. Бұл тәсіл Интернет жергілікті желілермен ауыстырылатын жабық инфрақұрылымға жатпайды, бірақ сервистердің бір бөлігі және жаһандық желіден қол жетімді.

Екінші тәсіл – виртуальизация. Виртуальизация оңай масштабтауға мүмкіндік береді. Виртуализацияның арқасында әрбір пайдаланушы болашақта кеңейту немесе кішірейту мүмкіндігімен қажетті қуатты ала алады. Барлық қызметтік процестер, бұл ретте, пайдаланушы үшін айқын. Қажетті жүйенің жұмысы үшін физикалық ресурстар әр түрлі дата-орталықтарда әртүрлі серверлерде бөлінуі мүмкін.

Үшінші тәсіл – Cloud Computing қызмет ретінде. Бұрын машиналар уақытына төлеп бос уақытын күту қажет еді. Cloud computing соған ұқсас жұмыс істейді, бірақ бұл тәсіл қазіргі заманға сай. Пайдаланушы үшін пайдаланылған ресурстар коммерциялық өнім беруші ұсынған жағдайда тұтынылатын және төленетін қызметтердің жиынтығы. Мысалы, HTTP REST API арқылы оларға кіру үшін хостингті қарастырайық. Пайдаланушы ыңғайлы интерфейс арқылы қол жетімді қажетті деректер көлеміне ие. Бұл ретте деректер физикалық серверлерде сақталады, Raid массивтердің көмегімен жоғалтудан қорғалады және аумақтық түрде бөлінген.

Төртінші тәсіл – қарапайымдылық және стандарттылық. Жаңа, толық бейімделген технология үшін өте маңызды Сапа. Бұлт барлық API және бұлтта ұсынылған хаттамалардың қарапайым қоңыраулары арқылы қол жетімді. Rest хаттамасы деректер бойынша барлық операцияларды орындауға болатын үлкен танымалдыққа ие болды. Көптеген басқа шешімдер, сондай-ақ қолданылады, әртүрлі бағдарламалау тілдері үшін осындай деректер жүйесін жазу үшін кітапханалар қол жетімді.

Бұлтты технологиялардың артықшылықтары ашылатын жағдайларды қарастырайық. Пайдаланушылар немесе ұйымдар үшін, ірі жеткізушілердің қызметтерін пайдаланған жағдайда, бұл қазіргі уақытта қажетті өнімділігі бар сенімді инфрақұрылымға қол жеткізуге арзан мүмкіндік. Коммерциялық жүйелердің қол жетімділігі, әдетте, 99.9% және одан жоғары деңгейде кепілдік беріледі,бұл жылына бір сағаттан артық бос тұруды білдіреді. Тағы бір маңызды сәт масштабталу бойынша үлкен мүмкіндіктер болып табылады. Мысалы,

бұлтты хостингті пайдалана отырып, ресурсқа немесе есептеуіш қуатқа барудың күрт көбеюімен іркіліс қаупі жоқ, өйткені барлық ресурстар динамикалық бөлінеді.

Осы тәсілдердің арқасында Cloud computing жаңа жобалар жасауға көмектеседі, олардың иелері болашақ қажеттіліктерді болжау қиындықтары тумайды.

NIST бойынша анықтама.

АҚШ – тың ұлттық технологиялар және стандарттар институтының NIST Definition of Cloud Computing құжатында бұлтты есептеулердің келесі анықтамасы беріледі (Cloud Computing): "Бұлтты есептеулер - бұл конфигурацияланатын есептеу ресурстарының бөлінетін пулына сұраныс бойынша (мысалы, желілер, серверлер, сақтау жүйелері, қосымшалар мен қызметтер) барлық жерде және ыңғайлы желілік қол жеткізуді ұсыну үлгісі, олар қызмет провайдерімен басқару және өзара іс-қимыл бойынша аз күш жұмсау арқылы тез берілуі және босатылуы мүмкін".

Бұл бұлтты есептеудің кешенді моделі бес негізгі сипаттаманы, үш сервистік модельді, төрт өрістету моделін қамтиды.

Бес негізгі сипаттамасы (Essential Characteristics):

Сұрау салу бойынша өзіне-өзі қызмет көрсету сервисі (On-demand self-service). Тұтынушыға есептеу ресурстары, серверлік уақыт және желілік қоймалар қажет болған жағдайда өзі сервиспровайдерден оның жұмысшылармен қатынамай өз бетінше сұрау арқылы ала алады.

Еркін (кең жолақты) желілік қатынау (Broad network access). Ресурстар мен сервистер жұқа және қалың клиенттердің гетерогенді платформаларын (мысалы, ұялы телефондар, ноутбуктер және КПК) пайдалануды қолдайтын стандартты механизмдер арқылы желі арқылы қол жетімділік.

Ресурстар пулы (Resource pooling). Олардың қажеттіліктеріне сәйкес, провайдердің есептеу ресурстары әртүрлі тұтынушылармен динамикалық тағайындау және әр түрлі физикалық және виртуальді ресурстарды қайта орнату мүмкіндігімен оларды көпше жалдау үшін пул түрінде ұйымдастырылған. Бұл ретте тұтынушы жалпы жағдайда сұратылған ресурстардың нақты орналасқан жерін білмейді және бақыламайды, алайда олардың жоғары деңгейде (мысалы, ел, штат немесе деректерді өңдеу орталығы) орналасуын анықтай алады. Мұндай ресурстардың мысалдары сақтау жүйелері, Есептеу мүмкіндіктері, жады, желінің өткізу қабілеті болып табылады.

Жылдам икемділік (Rapidelasticity). Есептеу ресурстары икемді, бірқатар жағдайларда сыртқы және ішкі қажеттіліктерге сәйкес жылдам масштабталумен автоматты түрде берілуі және босатылуы мүмкін. Тұтынушы үшін бұл ресурстар шексіз көлемде қолжетімді болады.

Өлшенетін сервис (Measured Service). Бұлттық жүйелер ресурсты пайдалануды2, оны сақтау көлемі, есептеу қуаты, Өткізу жолағы және пайдаланушылардың белсенді есептік жазбалары сияқты оған сәйкес метриктермен өлшей отырып, автоматты түрде бақылайды және оңтайландырады. Ресурстарды пайдалану провайдер үшін де, пайдаланылған сервистің тұтынушысы үшін де ашықтықты қамтамасыз ете отырып, мониторингілеуі, бақылануы және есептілікпен сүйемелденуі мүмкін

Үш сервистік модель бар (Service Models):

Бағдарламалық қамтамасыз ету қызмет ретінде – Cloud Software as a Service (SaaS). Тұтынушыға бұлтты инфрақұрылымда орындалатын провайдердің бағдарламалық қосымшалары беріледі. Қолданбалар түрлі клиенттік құрылғылардан немесе қолданушы жұқа интерфейсімен (мысалы, веб-интерфейсі бар электрондық пошта), немесе бағдарламалық интерфейс арқылы. Тұтынушы тораптар, серверлер, операциялық жүйелер, сақтау жүйелеріне өзгеріс енгізе алмайды және бақылмайды тек шектеулі пайдаланушылық конфигурациялық параметрлерді өзгерте алады.

Платформа қызмет ретінде – Cloud Platform as a Service (PaaS). Тұтынушыға провайдер бұлтты инфрақұрылым ішінд өрістетуге арналған құралдар ұсынылады және бағдарламалау тілдерін, кітапханаларды, қызметтер мен құралдарды пайдалана отырып қосымшаны дамытады немесе өрістетеді. Бұл аталған құралдарды басқа көздерден пайдалану мүмкіндігінде жоққа шығармайды. Тұтынушы бұлт инфрақұрылымын, соның ішінде желіні, серверлерді, операциялық жүйелерді немесе сақтау жүйелерін басқармайды және бақыламайды, бірақ кеңейтілген қосымшаларды және, мүмкін, қосымшалар жұмыс істейтін ортаның конфигурациялық баптауларын бақылайды.

Инфрақұрылым қызмет ретінде – Cloud Infrastructure as a Service (IaaS). Тұтынушыға процессорлық қуаттар, жады, желілер және операциялық жүйелер мен қосымшаларды қоса алғанда, еркін бағдарламалық қамтамасыз етуді өрістетіп, орындай алатын басқа да базалық компьютерлік ресурстар беріледі. Тұтынушы бұлтты инфрақұрылымды басқармайды және бақыламайды, бірақ операциялық жүйелерді, сақтау жүйелерін, өрістетілетін қосымшаларды бақылай алады және жеке желілік компоненттерді (мысалы, хостердің желілік экрандарын) шектеулі бақылауға ие болуы мүмкін.

Төрт өрістету үлгісі бар (Deployment Models):

Жеке бұлт (Private cloud).Бұлтты инфрақұрылым көптеген тұтынушылармен (мысалы, бөлімдермен) тұтас бір ұйымға қызмет көрсету мақсатында жұмыс істейді. Инфрақұрылым ұйымның өзі де, үшінші тарапқа тиесілі болуы, басқарылуы және бақылануы және ұйымның өзінде немесе сыртқы провайдерде болуы мүмкін.

Қауымдастық бұлты (Community cloud). Бұлтты инфрақұрылым жалпы қағидаттарды (мысалы, миссияны, қауіпсіздікке қойылатын талаптарды,

саясатты, сәйкестікке қойылатын талаптарды) бөлетін ұйымдардан тұтынушылардың белгілі бір қоғамдастығы үшін ғана жұмыс істейді. Инфрақұрылым қоғамдастықтан бір немесе бірнеше ұйымға, үшінші тарапқа немесе олардың кейбір комбинациясына тиесілі болуы және басқаруы, ұйымдардың өздерінде немесе олардан тыс болуы мүмкін.

Ашық бұлт (Public cloud). Бұлтты инфрақұрылым баршаға қолжетімді ретінде жұмыс істейді. Ол бизнеске, академиялық немесе үкіметтік ұйымдарға тиесілі және басқарылады, немесе олардың бір үйлесімі және провайдер меншігінде болады.

Аралас бұлт (Hybrid cloud). Бұлттық инфрақұрылым екі және одан да көп әр түрлі бұлттық инфрақұрылымдардың (жеке, жалпы немесе көпшілік), бөлек бірліктермен қалатын, бірақ деректер мен қосымшалардың (мысалы, олардың арасындағы жүктемені теңдестіруді қамтамасыз ету үшін бірнеше бұлттар) көтерілуін қамтамасыз ететін стандартталған немесе меншіктік технологиялармен бірге біріктірілген үйлесімі болып табылады.

1.1 Сервистік модель түрлері

Бұлттық жүйелерде есептеу қуаттарын беру нұсқалары бір-бірінен ерекшеленеді. Бұлтты технологиялар негізіндегі басты тәсілдердің бірі қызмет ретінде көрініс табуына байланысты, қызметтерді ұсыну нұсқаларының атауларына "as a service" сөз тіркесін қосу қабылданды, бұл аудармада "қызмет ретінде"дегенді білдіреді.

SaaS (Software as a service), немесе сервистер түріндегі бағдарламалар - нақты бағдарламалық қамтамасыз етуді, мысалы, корпоративтік жүйені, жазылу бойынша сервис түрінде пайдалану ұсынылатын нұсқа. Егер кәсіпорында ішкі Exchange сервері мен күнтізбелерді пайдалану мүмкіндігі болмаса, оны қашықтан сатып алуға болады.

PaaS (Platform as a service) - SaaS қарағанда, ол соңғы пайдаланушыға арналған, бұл опция әзірлеушілерге арналған. PaaS жағдайында бұлтта бағдарламалар, негізгі сервистер мен кітапханалардың жиынтығы жұмыс істейді, олардың негізінде өз қосымшаларын әзірлеу ұсынылады. Қызмет көрсетудің осы нұсқасының мысалы - Google AppEngine қосымшаларын жасау платформасы. Сонымен қатар, PaaS деп деректер қоры немесе коммуникация жүйесі сияқты күрделі жүйелердің жекелеген бөліктерін де түсінеді.

HaaS (Hardware as a service) - сервистер түріндегі кейбір базалық аппараттық функциялар мен ресурстардың берілуін білдіретін алғашқы терминдердің бірі. Серверді тікелей жалға алудың орнына виртуализация қолданылады. HaaS жағдайында, нақты аппараттық қамтамасыз ету ретінде ақпаратты сақтауға арналған орын сияқты физикалық ұқсас кейбір абстрактілі мәндер түсіндіріледі, оның эквивалентіндегі процессорлық уақыт немесе нақты CPU, өткізу қабілеті.

IaaS (Infrastructure as a service) - бұл термин HaaS орнына жаңа деңгейге көтере отырып келді деп саналады. Бұл термин компьютерлік инфрақұрылымды қызмет ретінде ұсыну деп аталады. Бұл жұмыста қуаттарды берудің осы нұсқасы қарастырылады.

CaaS (Communication as a service) - байланыс қызметтерін қызмет ретінде ұсыну. Байланыс қызметтері, әдетте, чат немесе жедел хабар алмасу қызметтері сияқты IP-телефонияны, поштаны немесе жедел коммуникацияларды білдіреді.

Әрбір модель соңғы пайдаланушыға ұсынылатын қызметтердің салыстырмалы сипаттамасы (1.1-кесте) кестеде келтірілген.

1.1 кесте – Бұлтты қызмет үлгілерін салыстыру

Түрі	Тұтынушы	Бұлт ұсынатын қызмет	Қызмет көрсету деңгейінің әрекет ету саласы	Баптау
SaaS	Соңғы пайдаланушылар	Дайын қосымша	Қосымшаның жұмыс уақыты. Қолданба өнімділігі	Ең аз немесе жоқ Нарық немесе өнім беруші анықтайтын мүмкіндіктер
PaaS	Қосымша иесі	Бағдарлама коды үшін орындау ортасы Бұлтты сақтау Интеграция сияқты басқа бұлтты қызметтер	Ортаның қолжетімділігі Ортаның жылдамдығы Қосымшаларға қолданылмайды	Ұсынылған қызметтер ішінде қосымшамалар деңгейінде жоғары өзгерту Төменгі деңгей сипаттамаларын өзгертуге мүмкіндік жоқ
IaaS	Қосымша иесі немесе АТ бөлім ОЖ және қосымша бағдарламаларға	Виртуальді сервер Бұлтты сақтау	Виртуальді сервердің қолжетімділігі Жұмысқа дайындау уақыты	ОЖ стандартталған виртуальді жинақтарында орнатылған қосымшалар үшін ең аз

	қолдау көрсетеді		Платформаға немесе бағдарламаларға қолданылмайды	шектеулер

1.2 Өрістету модель түрлері

Өрістету модельдері (жалпы немесе бөлінген, сондай-ақ ұйым ішінде немесе одан тыс орналасады) сәулет жобасын иелену және оны басқару, сондай-ақ қол жетімді баптау деңгейі ретінде анықталады. Әр түрлі

ресурстарды өрістету модельдері үш стандарт бойынша бағалануы мүмкін: құны, бақылау және масштабталу. Өрістетудің негізгі модельдері (суретте 1.1.) көрсетілген.

1.1 сурет – Өрістету модельдері

Жалпыға қол жетімді бұлт — бұл интернет арқылы берілетін компьютерлік қызметтер пулы. Ол әдетте нақты пайдалану немесе өлшенетін қызмет үшін төлем үлгісін пайдаланатын өнім берушімен ұсынылады. Жалпы қол жетімді бұлттық есептеулер келесі артықшылықтарға ие: төлем тек тұтынылған ресурстар үшін ғана жүргізіледі, икемділікті жылдам өрістету арқылы қол

жеткізіледі, қуаттарды жылдам масштабтау мүмкіндігі бар және барлық қызметтер қол жетімділіктің, бас тартымдылықтың, қауіпсіздіктің және басқарудың жақсартылған біркелкі сипаттамаларымен жеткізіледі. Жалпы қол жетімді бұлттың келесі түрлері бар:

– Ортақ пайдаланылатын жалпы бұлт. Ортақ пайдаланылатын бұлт тез енгізу, жаппай масштабтау артықшылығын және өндірісті ұйымдастыруға арналған төмен шығындарды қамтамасыз етеді. Ол сәулетті, теңшеу және қауіпсіздік деңгейі нарыққа бағдарланған ерекшеліктерге сәйкес өнім беруші жобалайтын және басқаратын жалпы ортада ұсынылады.

– Бөлінген жалпы бұлт. Бөлінген жалпы қол жетімді бұлт бөлінген инфрақұрылымды қоспағанда, бірлесіп пайдаланылатындарға ұқсас функционалдық мүмкіндіктерді қамтамасыз етеді. Қауіпсіздік, жылдамдық, кейде баптау мүмкіндігі ортақ қол жетімді бұлтқа қарағанда таңдалған. Оның сәулеті мен қызмет көрсету деңгейін жеткізуші анықтайды және оның құны көлеміне байланысты ортақ пайдаланылатын бұлтқа қарағанда жоғары болуы мүмкін.

Жеке бұлт — бұл нақты кәсіпорынмен анықталатын, жобаланатын және бақыланатын қызметтердің стандартты жиынтығы ретінде ұсынылатын компьютерлік ресурстар пулы.

Жеке бұлтқа жиі ескірген қосымшалардың болуымен немесе өнімділікке қойылатын жоғары талаптармен және реттеуші нормаларға бақылау қажеттілігінен қолданысқа ие. Мысалы, банктер мен үкіметтік мекемелер жалпы қол жетімді бұлт қолдана алмайды себебі олар толық жүргізілген әрекеттерді бақылай алмайды сондықтан жеке бұлтпен қолдануға қажеттілік туындайды. Жеке бұлттың келесі түрлері бар:

– Дербес орналастырылған жеке бұлт. Дербес орналастырылған жеке бұлт сәулеті мен операцияларды бақылау тұрғысынан артықшылықтары бар, онда жұмысшы мен жабдықтарға қолда бар инвестициялар пайдаланылады және ол компания ішінде жобаланатын, орналастырылатын және басқарылатын бөлінген жергілікті ортаны қамтамасыз етеді.

– Орналастырылған жеке бұлт. Орналастырылған жеке бұлт-бұл компанияның ішінде жобаланатын, ал одан тыс жерлерде орналасқан және басқарылатын бөлінген орта. Онда аутсорсинг артықшылықтарымен қызметті және сәулеттілік жобаны басқару артықшылықтары үйлеседі.

– Құрылғы негізіндегі жеке бұлт. Құрылғы негізіндегі жеке бұлт — бұл өнім берушіден сатып алынатын және қызмет көрсетушіге және нарыққа бағытталған функциялармен және сәулеттң бақылаумен жобаланған бөлінген орта. Бұл орта ұйымның ішінде орналасады және ішкі немесе сыртқы басқаруы болады. Онда ішкі қауіпсіздік және бақылау жүйесінің артықшылықтарымен өрістету кезінде алдын ала реттелген сәулетін және төмен тәуекелдерді пайдаланудың артықшылықтары үйлеседі.

1.2 кесте – бұлт өрістету модельдерін салыстыру

Өрістету түрі	Орналасу орны	Жалпы немесе бөлінген	Сәулет басқармасы	Масштабталуы	Қажетті инвестициялар
Ортақ пайдаланылатын Жалпы қол жетімді бұлт	Сыртқы	Жалпы	Жеткізуші немесе нарық	Ең төменгі шектеулер	Нақты пайдалану үшін төлем
Бөлінген жалпы бұлт	Сыртқы	Ішінара немесе толық бөлінген	Жеткізуші немесе нарық	Келісім-шартпен шектелген	Нақты пайдалану үшін төлем
Дербес орналастырылған жеке бұлт	Ішкі	Толығымен бөлінген	Дербес	Күрделі инвестициялармен шектелген	Бұлт жасау, жалпы қызметтер
Орналастырылған жеке бұлт	Сыртқы	Толығымен бөлінген	Дербес	Күрделі инвестициялармен шектелген немесе келісім-шартпен шектелген	Келісімшартқа байланысты, капиталға әсер етуі немесе әсер етпеуі мүмкін
Құрылғы негізіндегі жеке бұлт	Ішкі	Толығымен бөлінген	Жеткізуші	Ұсыныспен шектелген	Келісімшартқа байланысты, капиталға әсер етуі немесе әсер етпеуі мүмкін

1.3 Даму бағыты

Қазіргі заманда әлем компанияларының 60% IT-бюджетінің 30% - ын бұлтқа жұмсайды. Бүгінде 57% компания өзінің бұлтын да, вендорлардың бірінің бұлтын да пайдаланғанда гибридті бұлттардың үлесіне тиеді. Соңғы жылы гибридті бұлттардың үлесі 3 есе өсті, бұл сарапшылардың пікірінше, бизнес бұлт

сервистерін түпкілікті және сөзсіз игере бастағанын көрсетеді. Мысалы, Amazon бұлтының пайдаланушылары АҚШ-тың 2000-нан астам мемлекеттік органдары болып табылады, және мұндай консервативті құрылымдар осындай қадамға барлық артышылықтар мен кемшіліктерді ескере отырып шешкені мәлім.

Қазақстанда бағдарламалық қамтамасыз етуді жалға алу (SaaS), виртуальді дата-орталық (IaaS) қызметтері және физикалық жабдықтарды жалға алу сияқты қызметтер сенімді сұранысқа ие. Жалпы, бүгінгі күні IaaS-қа қазақстандық бұлтты нарықтың басым үлесі тиесілі, бірақ сұраныс құрылымы SaaS жағына қарай өзгеруі мүмкін. Бұл жалпы әлемдік тренд. Қазір нарықтың 36% таза бұлтты қызметтерге тиесілі, салыстыру үшін 2015 жылы бұл көрсеткіш 29% – ды құрады. Өсім бар, бірақ бұл сегментте қазақстандық нарық жалпы әлемдік көрсеткіштен біршама артта қалып отыр: Gartner деректері бойынша, 2019 жылы SaaS-та әлемдік бұлтты сервистер нарығының 44% - ға жуығы келді. Қазақстандық нарықтың әлеуеті мұнда әлі іске асырылмаған деп болжауға болады.

Бәрі алда екендігіне мынадай сандар да айтылады: Қазақстандық нарық өсуге өте үлкен мүмкіндіктер бар себебі, отандық қызмет берушілер бұлтты қызметтерге деген сұраныстың тек 27% - ын ғана қанағаттандырады. Сонымен қатар, дата-орталықтар – бұл сандық экономиканың ең кең түсінігіндегі база ғана емес – 5G, IoT, Big Data, VR, AI және Smart City. 2022 жылға қарай, Gartner бағалауы бойынша, әлемдік бұлтты нарық екі есе өседі – $331 млрд.

Мамандар IT-инфрақұрылымды өрістету жеделдігін бұлтты шешімдердің пайдасына басты дәлелдердің бірі деп санайды. Кіші және орта бизнес сегментінде жұмыс істейтін компаниялар үшін IT-инфрақұрылымын іске қосудың орташа мерзімі үш айдан жарты жылға дейін. Бизнестің даму қарқынын ескере отырып, бұл өте ұзақ уақыт алатыны айқын, сонымен қатар үлкен шығындарды талап етеді. Және де, өндірістік процеске жасанды интеллект пен машиналық оқытуды енгізу перспективалары IT мамандардан кәсіби даярлаудың жоғары деңгейін талап етеді. Егер бұлтты провайдерлер мамандануына байланысты өз қызметкерлерінің құзыретін арттыру үшін үнемі жұмыс істейтін болса, онда басқа компанияларда оған үлкен шығындар орынсыз деп есептеледі.

Қазақстандағы KPMG және "Зерде" ұлттық инфокоммуникация холдингі зерттеу деректеріне сәйкес бұлтқа жұмсалатын шығындардың орташа үлесі IT-ға арналған бюджеттің 15% - ға жуығын құрайды. KPMG-дағы IT саласындағы мамандар екі-үш жыл ішінде компаниялардың бұлтты технологияларды енгізуден қауіптенетін себептерінің өзгергенін айтады. Бұрын 75% жағдайда олар деректерді жоғалтумен байланысты реттеу мен қауіптердің шешілмеген мәселелері туралы айтты ал, 25% бұлтты енгізу қиындықтарына байланысты екендігін жеткізді. Бүгінгі таңда 54% - да бизнес компанияның ландшафтындағы интеграция проблемаларынан қауіптенеді, 53% – ы деректерді жоғалту мен

жекелену мүмкіндігі туралы алаңдатады, 52% - ы реттеушілермен қиындықтарға, 40% - ы басқару күрделілігіне сілтеме жасайды.

Сауалнама нәтижелері реттеу мәселелері әлі де IT нарығына қатысушылар мен бизнес өкілдерін алаңдататынын көрсетті. ҚР заңнамасында "бұлт" немесе "бұлтты технологиялар" заңды терминдері жоқ, бірақ бұл қызметтің осы саласы реттелмейтіндігін білдірмейді. Керісінше, нақты регламенттеудің болмауы тәсілдердің алуан түрлілігін тудырды. Бұлт қызмет ретінде де, байланыс құралы ретінде де, ақпараттық жүйе ретінде де қарайды – әрбір тәсілде банк жүйесі, сақтандыру нарығы немесе мысалы, өнеркәсіптік өндіріс туралы әңгіме болып отырғанына байланысты өзінің салалық реттеуі бар.

Провайдер бұлтқа өтудің пайдасына басты дәлелдердің бірі шығындарды қысқарту мүмкіндігін тек шын мәнінде қажетті шешімдер үшін ғана төлеуге болады деп атайды. Сарапшылардың айтуынша, компанияларда өз жабдықтарын орташа кәдеге жарату 30% - ды құрайды, яғни сатып алынған қымбат бағалы "темір" және шешімдер тек өз мүмкіндіктерінің үштен бір бөлігіне ғана жұмыс істейді, ал деректерді өңдеу орталықтарында көрсеткіш 90% - ға жетеді.

Деректерді жоғалту қаупі бар. Бұлт арқылы бизнес өз процестерін неғұрлым тиімді етуге ұмтылады, бірақ бұлт, ашық немесе жеке, қақтығыстардан сақтандырылмаған – бұл Dropbox, және Bitrix, және Tesla тап екенін сарапшылар ескертеді. Мүмкін тәуекелдердің қатарында-бағытталған және DDoS-шабуылдар, деректердің ағып кетуі.

Егер инциденттер тәуекелін бизнес деректер ретінде қабылдауы керек болса, онда пайдаланушылармен қарым-қатынасты ойластыру қажет. Деректер ағынының өзі бірнеше клиенттердің кетуінің себебі болуы мүмкін, бірақ егер компания болған оқиға туралы жоққа шығаруға тырысса және бұл туралы белгілі болса, беделді және қаржылық шығындар әлдеқайда үлкен болуы мүмкін.

Кез келген бастамамен бірге жүретін тәуекелдерге қарамастан, ірі ұлттық компаниялар мен кіші және орта бизнес кәсіпорындарының активінде қызметтердің бір бөлігін бұлтқа аударудың табысты істер пайда болды. Мәселен, Air Astana бұлтқа бортсеріктер, техникалық және қызмет көрсетуші жұмысшылар үшін қосымшалар енгізілді. "Қазпочта" АҚ-да үш жыл бұрын жеке байланыс орталығын құруды шешті, бірақ оны жабдықтау және қызметкерлерді оқыту шығындары өте жоғары болды, бұл сервисті аутсорсингке беру туралы шешім қабылданды. Осындай модельді деректерді өңдеу орталығы мен баспа құрылғылары паркі үшін қолдану жоспарланып отыр. Өз ЦОД-ын құру Mykhat-да, сандық курьерлік компания үшін шығын деп саналды. Кейінен, "Қазтелепорт" провайдерімен ынтымақтастықтың арқасында мәліметтерді сақтау мәселесін шешуге, құжат айналымын ішінара автоматтандыруға қол жеткізілді.

Сандық бәсекеге қабілеттіліктің әлемдік рейтингісінде (IMD World Digital Competitiveness Ranking 2019) Қазақстан Ресейді (38-ші орын) және Украинаны (60-шы орын) басып озып, 35-ші орынды иеленді. Алайда, Қазақстанда әзірге

мынадай көрсеткіштер бойынша төмен бағалар бар: үлкен деректер мен талдауларды пайдалану, компаниялар мен мемлекеттік-жеке меншік әріптестіктің икемділігі. Естеріңізге сала кетейік, рейтингте елдердің бизнесті, мемлекеттік басқару мен қоғамды трансформациялаудың негізгі бағыттаушы ретінде сандық технологияларды зерттеу және енгізу қабілеті мен дайындығы бағаланады.

1.4 Бұлтты сервистерге төнетін қауіптер.

Cloud Security Alliance (CSA), бұлтта қорғау әдістерін ілгерілететін коммерциялық емес салалық ұйым өзінің басты қауіптерінің есебін көрсетті. CSA бұлттағы қауіпсіздіктің ең маңызды қатерлері туралы сарапшылардың келісілген пікірін көрсетеді және ортақ бұлт ресурстарын бірлесіп пайдаланудан және талап бойынша көптеген пайдаланушылардың жүгінуінен туындайтын қатерлерге негізгі назар аударады. Есеп, бұлт пайдаланушылары мен бұлтты қызметтерді жеткізушілерге ең қауіпті тәуекелді төмендету стратегиясын енгізуге көмектесу мақсаты бар.

1.4.1 Деректерді жоғалту. Кіріу мәліметтерін таңдау. Деректерді жоғалту.

Деректерді жоғалту — (Data Loss) - әр түрлі факторлардың, кездейсоқ немесе әдейі әрекеттердің әсерінен ақпараттың зақымдануы немесе жоғалуы. Деректерді олармен жұмыс істеу кезінде, сондай-ақ ақпаратты компьютерде, серверде немесе RAID массивтерінде сақтау кезінде жоғалтуға болады.

Деректерді жоғалту (Data Loss) нәтижесінде болуы мүмкін:

Ақпараттың тұтастығын бұзу (бағдарламалық қамтамасыз етудің бұзылуы).

Ақпарат тұтастығының бұзылуы қалпына келтіру процедурасын орындамай, ақпаратты оқу/көшіру мүмкін емес,ол деректердің бүлінуін білдіреді. Бүтіндік бұзылғанда барлық деректерді немесе олардың бөліктерін жоғалту қаупі, сондай-ақ бүкіл компьютерлік жүйенің жұмыс істеу қабілеттілігіне қауіп туындайды.

Жиі қымыскердің ену кеісірінен ақпараттардың бүтіндігі бұзылады. Бірқатар зұлымдық әрекеттер қылмыскерді алға қойған мақсатқа алып келеді. Бұл компанияда қызметкерлерінің зиянды қызметі, киберқылмыскерлердің шабуылдары, басқа да жағдайлар болуы мүмкін. Бүтіндіктің бұзылуына бағдарламалық жасақтаманың ақаулығы әкелуі мүмкін. Қате зиянды бағдарламалардың әсерінен, қолданбаларды дұрыс орнатпаудан, бағдарламалық өнімдерді сәтсіз жаңартудан, операциялық жүйені орнатқан кезде қате пішімдеуден немесе жаңартқан кезде қатеден туындауы мүмкін.

Жабдықтың ақаулықтары.

Жабдықтың ақаулығы пайдаланушының немесе кез келген компанияның деректерін толық жоғалтуыға әкеп соғуы мүмкін. Ол әдейі немесе қаскүнемдің белгілі бір әрекеттерінің нәтижесінде пайда болады. Жабдық ақаулығының бірнеше себептері бар, мысалы, табиғи апаттар. Компьютерлік құрылғылар осы табиғи апат оның ішіде: су тасқыны, дауыл, найзағай, өрт және т.б. зардап шегуі мүмкін.Осы жағдайлар құрал-жабдықтардың жұмыс істемеуіне немесе деректердің толық жоғалуына әкеп соғады. Кернеудің секіруі, қоршаған ортаның температурасының жоғарылауы дербес компьютерлердің немесе серверлердің компоненттерінің тұтануына, қатты дискінің зақымдануына әкеледі. Жабдық вандалдардың кінәсіненде жарамсыз болуы мүмкін. Сонымен қатар қасақана басқа адамның заңсыз кіруі немесе бәсекелестері адамдар жалдау арқылы жүзеге асыралады. Компьютерлік техникаға қызмет көрсететін қызметкерлер немесе сыртқы қызметкерлер пайдакүнемдік мақсаттан, кек алуы мақсатында зиян келтіруі мүмкін. Сонымен қатар, жабдықтың ақаулығы оның жекелеген тораптарының жұмысындағы проблемалардан немесе істен шығуы себебінен туындауы мүмкін.

Кіріу ақпараттарын таңдау.Басқару және қашықтан кіру интерфейстері

Қашықтықтан қол жеткізу хаттамалары жүйелік администратордың жұмысын жеңілдетеді және оған қашықтан құрылғыларды басқаруға мүмкіндік береді. Кең таралған құралдардың арасында-Telnet, RSH, SSH және RDP сияқты қашықтан қосылу протоколдары бар. Көбінесе жүйелік администраторлар бұл үшін жалпыға қолжетімді бағдарламалық қамтамасыз етуді пайдаланады: Radmin, Ammyy Admin және ұқсас. Бұл сырттан жасалатын бұзушыға есептік деректерді таңдауға шабуыл жасауға мүмкіндік береді.

Мұндай шабуыл ешқандай ерекше білім және дағдыларды талап етпейді: көп жағдайда интернетте оңай табуға болатын есептік деректер мен сөздіктерді таңдау үшін ноутбук, бағдарламалар жеткілікті. Шабуылды IP мекен-жайлары бойынша жүргізуді қиындатуы мүмкін. Бұл жағдайда тәртіп бұзушы басқа жолдарды табады. Мысалы, желіде басқа тораптарды бұзады және шабуылды өзінің мекен-жайынан емес, компрометирленген түйіндерден дамытуға тырысады. Сүзгілеудің басқа да әдістері бар.

SSH және Telnet-тен құпия сөз ретінде root:root, root:toor, admin:admin, test:test комбинациясын кездестіруге болады. Кейбір жағдайларда ең жоғары артықшылық кезінде құпия сөзді енгізбей қол жеткізуге болады.

RDP кіру үшін локальды немесе домен есептік жазбалары қолданылады.Жиі бұл Administrator:P@ssw0rd, Administrator: 123456, Administrator:Qwerty123, сондай-ақ бос парольмен есептік жазба болады.

1.4.2 Бағдарламалық қамтама осалдықтарын пайдалану.

Біздің статистикамыз бойынша, ескірген нұсқаларды пайдалану — қауіпсіздіктің ең көп таралған кемшіліктерінің бірі. Әдетте, пентестердің шеңберінде кодты алыстан орындауға мүмкіндік беретін БҚ осалдықтарды пайдалану жүргізілмейді, өйткені осындай шабуылдар мысалы, буферді асыра толтыруға бағытталған жүйелерге қызмет көрсетуден бас тартуын тудыруы мүмкін. Қылсымкер үшін бұл шарт кедергі болмайды, бірақ оның негізгі мақсаты болуы мүмкін. Сонымен , әртүрлі жүйелердің ескірген нұсқаларының және олардың осалдықтарының кейбір таралған мысалдары:

– Windows Server 2003 SP1, SP2 (CVE-2012-0002);

– nginx 1.3.11 (CVE-2013-2028);

– PHP 5.3.8, 5.3.28, 5.5.1 және басқа да көптеген нұсқалар (CVE-2014-3515, CVE-2011-3379, CVE-2013-6420), ProFTPD FTP Server 1.3.3a (CVE-2011-4130, CVE-2010-4221), OpenSSH Server 4.3 (CVE-2006-5051, CVE-2006-5052). Осы уақытқа дейін белгілі осалдығы бар Windows XP-ді (CVE-2008-4250) кездестіруге болады.

Мұндай осалдықтарды жиі пайдалану шабуылдаушыға ерекше білім мен дағдыларды талап етеді.Мысалы, жеке эксплоитті әзірлеу үшін. Сонымен қатар, "қораптан" немесе нақты жағдайларға бейімделу үшін ең аз өзгерістермен пайдаланылуы мүмкін жалпы қол жетімді, сондай-ақ коммерциялық эксплоиттер бар.

Бірқатар жобаларда біз қауіпті Heartbleed осалдығын (CVE-2014-0160) пайдалануды көрсеттік. Егер қызмет SSL қосылымдарын қолдаса немесе торапта *nix-секілді ОЖ пайдаланылса, OpenSSL кітапханасының осал нұсқасы серверлік үдерістің жадын осы мысалда — веб-серверді оқуға мүмкіндік береді. Мұндай жад учаскелерінде аса маңызды деректер: пайдаланушылардың есептік деректері, пайдаланушы сессиялары, кіру кілттері және т.б. ашық түрде болуы мүмкін. Шабуыл жүргізу және жад учаскелерін талдау нәтижесінде, атап айтқанда, Пайдаланушының паролі алынды.

1.4.3 DDoS-шабуылдар.

DDoS-шабуыл сызбалық түрде келесі көрініске ие: зардап шегуші ретінде таңдап алынған серверге әлемнің түрлі нүктелерінде орналасқан компьютерлерден көптеген жалған сұратулар келіп түседі. Нәтижесінде сервер өзінің бүкіл ресурстарын осы сұратуларды өңдеуге жұмсайды да, қарапайым пайдаланушылар үшін толық дерлік қолжетімсіз болып қалады. Жалған сұратулар жіберілген компьютерлердің пайдаланушылары өздерінің машиналарының хакерлер тарапынан қолданылғанын білмеуі де мүмкін. Осы компьютерлерде зиянкестер тарапынан орнатылған бағдарламалар «зомби» деп аталады. Компьютерлерді «зомбилендірудің» қорғалмаған желілерге рұқсатсыз

кіруден троян-бағдарламаларды қолдануға дейін баратын көптеген жолдары белгілі. Бұл дайындық кезеңі зиянкес үшін ең күрделі кезең болып табылады деуге болады.

Қолданбалы деңгейдегі DDoS-шабуылдардың түрлері (Application layer DDoS) қолданбалы немесе 7-ші деңгейдегі шабуылын есептеу қуатын талап ететін көптеген сұраныстарды жіберу болып табылады. Бұл сыныпқа HTTP-флуд және DNS-флуд шабуылдары да кіреді.

HTTP-флуды

HTTP-флуды әдетте белгілі бір мақсатқа қарсы жүзеге асырылады, соның салдарынан мұндай шабуылдың алдын алу өте қиын. Онда зиянды пакеттер пайдаланылмайды, ол бот-желіге көбірек сүйенеді.

DNS-флуды

Шабуылдың бұл түрінде мақсатты құрбан DNS сервері болып табылады. DNS сервері қол жетімсіз болса, тиісті серверді таба алмайсыз. DNS-флуд-бұл бот-желіде орналасқан және UDP шабуыл класына жататын көптеген зомби іске қосылған симметриялық шабуыл. Бұл шабуыл спуфингті жеңілдетеді.

DDoS желілік деңгейі (Network layer DDoS)

Бұл секундына гигабиттерде (Гбит/с) немесе секундына пакеттерде (PPS) өлшенетін өте ауқымды шабуылдар. Мұндай DDoS-шабуылдардың түрі SYN-флуд пен UDP-флудқа бөлінеді.

SYN-флуды

Бұл сұрауларға жауап беру мүмкін болмайтын кезде,серверге қосылу сұраулар ағынын жасайды. Бұл жерде әрбір сервер порты SYN-пакеттермен, соның есебінен серверде қосылу кезегі толып кетеді. Бұл жағдайда SYN-ACK пакеттері елеілмейді, соның арқасында клиенттен растауды күтетін жартылай ашық қосылыстар пайда болады.

UDP-флуды

UDP сервері әр портқа сұрау салады. Бұл жағдайда сервер "адресат қолжетімсіз" пакеттерімен жауап береді, нәтижесінде шабуылдау жүйесі шамадан тыс жүктеліп, жауап бере алмайды.

Амплификация (күшейту) — бұл DDoS-шабуылдарды өткізу жолдарын күшейту үшін қолданылатын әдіс. Сұрау салудағы IP-мекенжайды ауыстыру арқылы қылмыскер өзінің шабуылының тиімділігін 70 есе арттыра алады. Күшейту коэффициенті сервер түріне байланысты өзгеруі мүмкін. Мысалы, monlist командасы жиі NTP DDoS-шабуылдар үшін қолданылады. Бұл команда зиянкестерге NTP соңғы 600 клиенті туралы мәлімет жібереді. Яғни, залалданған компьютерден аз сұраныс болса, үлкен UDP ағыны жіберіледі. Мұндай шабуыл ботнетті пайдалану кезінде үлкен ауқымға ие болады.

1.4.4 Әлеуметтік инженерия.

Әлеуметтік инженерия — мақсатты шабуылдардың ең көп таралған әдістерінің бірі. Ол қызметкерлердің қауіпсіздік мәселелеріндегі тәжірибенің жетіспеушілігін пайдалануына әкеп соғады. Қылмыскер телефонмен сөйлесу немесе жеке хат алмасу арқылы ресурстарға қол жеткізу үшін деректерді шығаруы мүмкін.

Банк қызметкерлерінің бірімен телефон арқылы сөйлескен әлеуметтік инженерияның үлгісін келтіреміз. Қызметкер фишингтік хаттарды алғашқы тарату нәтижелері бойынша әңгімелесу үшін таңдады. Бұл хаттың сілтемесі бойынша ауысып қана қоймай, өзінің корпоративтік желісінің администраторы ретінде оны қабылдап, сарапшымен хат алмасуға кіріскен алушылардың бірі болды.

Біздің сарапшымыз администратор болып, пошта таратылымындағы жұмыс істемейтін сілтеме проблемасын шешуді ұсынды. Телефонмен сөйлесу төрт минутқа созылды және осы уақыт қойылған мақсатқа жету үшін жеткілікті болып шықты, осы арқылы қызметкердің жұмыс станциясына және доменнің ресурстарына қол жеткізіп алады.

1.4.5 Зиянды бағдарлама.

Зиянды бағдарламаларға компьютерлік техникаға рұқсатсыз кіретін кез келген бағдарламалық қамтамасыз ету жатады. Мұндай қосымшалар тікелей немесе жанама зиян келтіреді — мысалы, компьютер жұмысын бұзады немесе пайдаланушының жеке деректерін ұрлайды.Зиянкестер екі негізгі мақсаттарды іске асыру үшін құрылады. Олардың бірі құрбанның компьютеріне енгізуден пайда табу. Мысалы, қылмыскер компьютерді басқару мүмкіндігіне қол жеткізеді, құпия ақпаратты ұрлайды, қорқытып алушылықты жүзеге асырады.Екінші топқа келетін болсақ, ол материалдық пайдаға байланысты емес. Зиянды кодты жазу бағдарлама жасаған автордың өз іс-әрекеттерінде, әдеттегі бұзақылықпен немесе қалжың ниетімен көрініс болуы мүмкін.

Microsoft корпорациясы зиянды бағдарлама ретінде-бұл жеке компьютерге немесе тұтас желіге, серверге зиян келтіру мақсатында әзірленген кез келген БҚ. Бұл вирус, троян немесе тыңшылық бағдарламаның түрі болып табылады ол әзірше маңызды емес.

Зиянды бағдарламалардың түрлері

Төменде зиянды бағдарламалардың негізгі түрлері көрсетілген.

Ботнет агенттері. Ботнет деп зиянкестерден команда алатын заладанған компьютерлер тобы аталады.Бұл командаларды қабылдау және орындау үшін тиісті зиянды бағдарламаға жауап береді. Мұндай желі бірнеше бірліктен

миллион компьютерге дейін болуы мүмкін, ол сондай-ақ зомби-желі деп аталады.

Эксплойттар — бағдарламалық қамтамасыз етуде осалдықтарды пайдалануға арналған хакерлік утилиттер.

Бекдорлар — компьютерге қашықтан қосылу және оны басқару бағдарламалары.

Компьютерлік вирустар. Вирус деп басқа қосымшаларға өз кодын енгізетін бағдарлама деп аталады, сондықтан жұқтырылған объектіні әрбір іске қосу кезінде бұл код орындалады.

Руткиттер — зиянды қызметті жасыру құралдары мысалы, басқа қолданбалар қалаусыз БҚ тиесілі файлдарды анықтай алмайды.

Желілік құрттар-компьютерлік желілер бойынша өз бетінше таратуға қабілетті, әртүрлі функционалдық жүктемесі бар зиянды бағдарламалар.

"Троян"— әртүрлі бағыттағы зиянды объектілердің кең класы, олар әдетте өз тарату механизмі жоқ, яғни файлдарды жұқтыруы немесе өз көшірмелерін желі арқылы көбейте алмайды. Атауы олардың енуінің ерте тактикасынан пайда болды - легитимдік бағдарлама түрінде немесе оған жасырын қосымша ретінде.

Ерекше топқа бопсалаушылар мен шифролау бағдарламасын (ransomware) бөліп көрсетуге болады. Мұндай зиянды бағдарламалардың жұмыс сценарийі олар қандай да бір тәсілмен пайдаланушының оның деректеріне кіруін оқшаулайды және блоктан шығару үшін сатып алуды талап етеді.

Зиянды бағдарламалардың шабуылдары интернеттің барлық пайдаланушыларына таралады. Әсер ету мақсатында зиянкестердің түріне байланысты: бұзақы, ұсақ ұры немесе киберқылмыскер. Бір жұқпа компьютермен қалыпты жұмыс істеуге кедергі келтіреді, екіншісі-қаржылық шығындарға әкеледі, үшіншісі-коммерциялық құпияны құрайтын мәліметтердің жайылып кетуімен аяқталады.

Соңғы жылдары зиянды бағдарламалардан әртүрлі компаниялар мен ұйымдар жиі зардап шекті — бірінші кезекте өзінің төлем қабілеттілігіне байланысты. Типтік шабуылдар жасалды, мысалы, бухгалтерлік деректер базасын шифрлау және бизнес үшін өте маңызды осы ақпаратты қалпына келтіру үшін оның ақша соммасын төлеу негізгі талап болып табылады. Эксплойттар, трояндар мен құрттардың шабуылдарына банк карталарының деректерін қоса алғанда, клиенттер мен пайдаланушылар туралы ақпаратты теріске шығарады, бұл қаржыны, дерекқорларды, басқа да корпоративтік ақпаратты жоғалту қаупін төндіреді.

1.4.6 Шабуылдар туралы статисикалық мәліметтер

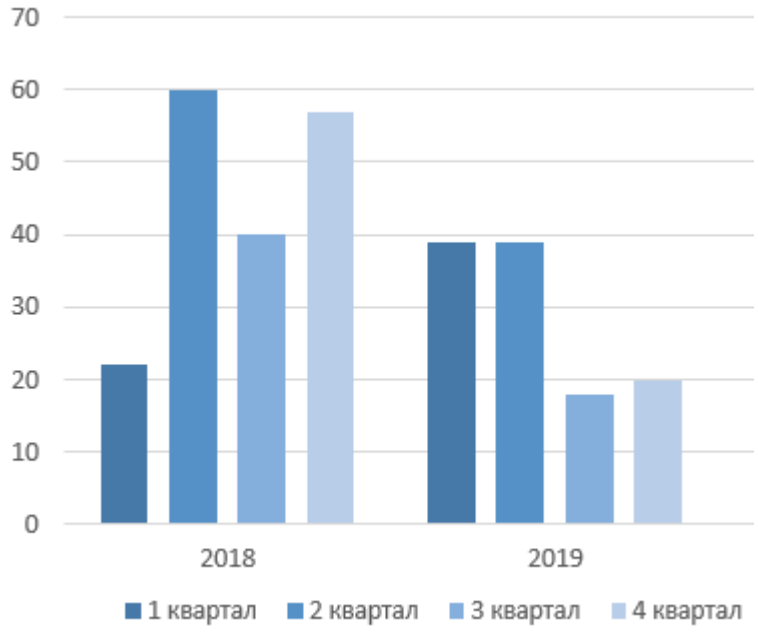
2018-2019 жылдар аралығында болған шабуылдар стаистикасы және қаншалықты қарқынды дамуын анықтау. Статистикалық мәліметтер Positive Technologies және Kaspersky компания жылдық қортындыларынан алынды.

Деректерді жоғалту. Кіріу мәліметтерін таңдау.

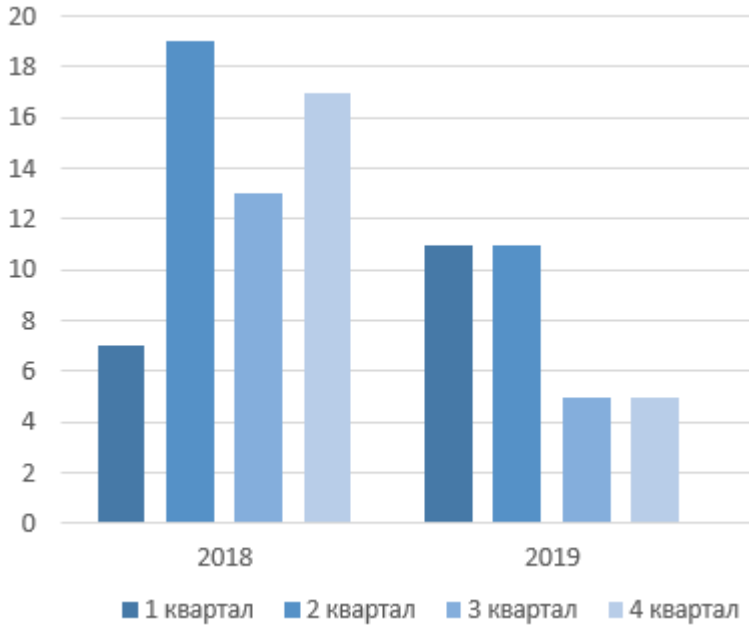
Құпия корпоративтік ақпаратты ұрлау — кез келген IT-инфрақұрылымында ұйымдарды әрдайым қорқытады, бірақ бұлтты модель "шабуылдардың жаңа, елеулі магистральдарын" ашады. "Егер көптеген жалға алынған бұлт деректер қоры дұрыс ойластырылмаса, онда бір қолданушы қосымшасында алынған бұлт тек қана осы қолданушының деректеріне ғана емес, сонымен қатар қалған бұлт пайдаланушыларының деректеріне қол жеткізуді бұзушыларға жол аша алады".

Бұлтта сақталған деректерді зиянкестер ұрлауы немесе басқа себептермен жоғалуы мүмкін,. Егер бұлт провайдері сақтық көшірудің тиісті шараларын енгізбесе, деректерді провайдердің өзі алып тастауы мүмкін немесе олар өрт немесе табиғи апат кезінде зардап шегеді. Екінші жағынан, тапсырыс беруші, кенеттен шифрлау кілтін жоғалтса, сондай-ақ өз деректерін жоғалтқанша, деректерді бұлтқа түсіргенге дейін шифрлау қажет.

Бұлт ортасында бұзғыш ұрланған тіркеу ақпаратын пайдаланушыларды зиянды сайттарға қайта бағыттау үшін қолдан жасай алады. Ұйымдар өзінің тіркеу деректерін басқа қызметкерлерге таратуға және барлық сервистер үшін бірдей парольдерді пайдалануға тыйым салған жөн. Сондай-ақ, тәуекелді төмендету үшін сенімді, екі факторлы аутентификацияны енгізу қажет.



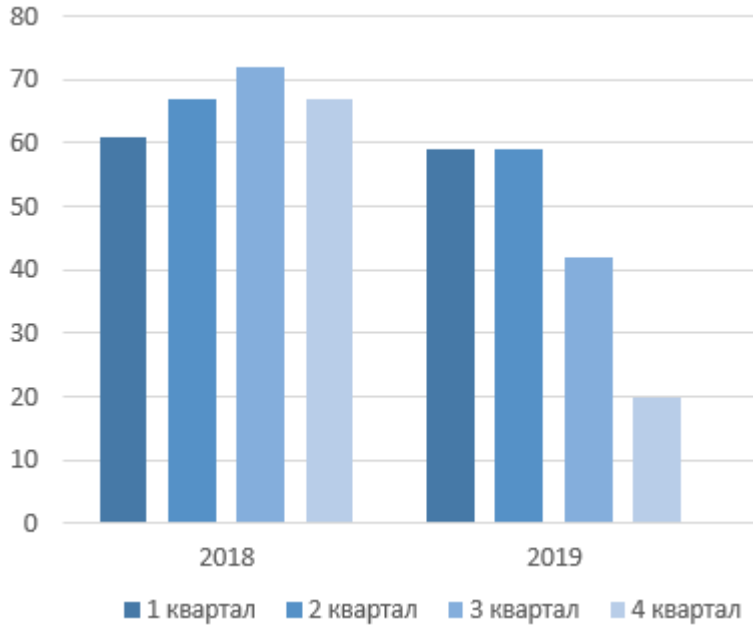
1.2 сурет – Шабуылдар саны



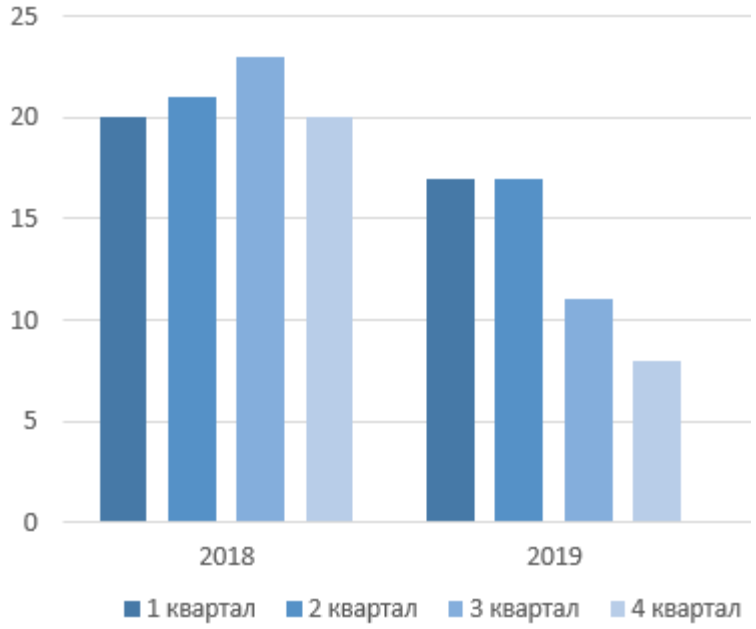
1.3 сурет – Шабуылдар үлесі

Қорғау тетіктерінің кемшіліктері мен бағдарламалық қамтама осалдықтарын пайдалану

Бұлтты қызметтермен басқару және өзара іс-қимыл жасау үшін тапсырыс берушілер пайдаланатын БҚ немесе API әлсіз интерфейстері бірқатар қатерлерді ұйымдастыруға ұшырайды. Бұл интерфейстер дұрыс жобалануы тиіс және бұлттық қызметтердің қажетті қорғанысы мен дайындығын қамтамасыз ету үшін аутентификацияны, қолжетімділікті басқару мен шифрлауды міндетті түрде қамтуы тиіс. Сондай-ақ ұйымдар мен бөгде мердігерлер қосымша қызметтерді ұсыну үшін бұлтты интерфейстерді жиі пайдаланады, бұл оларды неғұрлым күрделі етеді және тәуекелді арттырады, өйткені тапсырыс беруші өзінің тіркеу деректерін осындай мердігерге қызметтерді көрсетуді жеңілдету үшін хабарлау қажет болуы мүмкін.



1.4 сурет – Шабуылдар саны

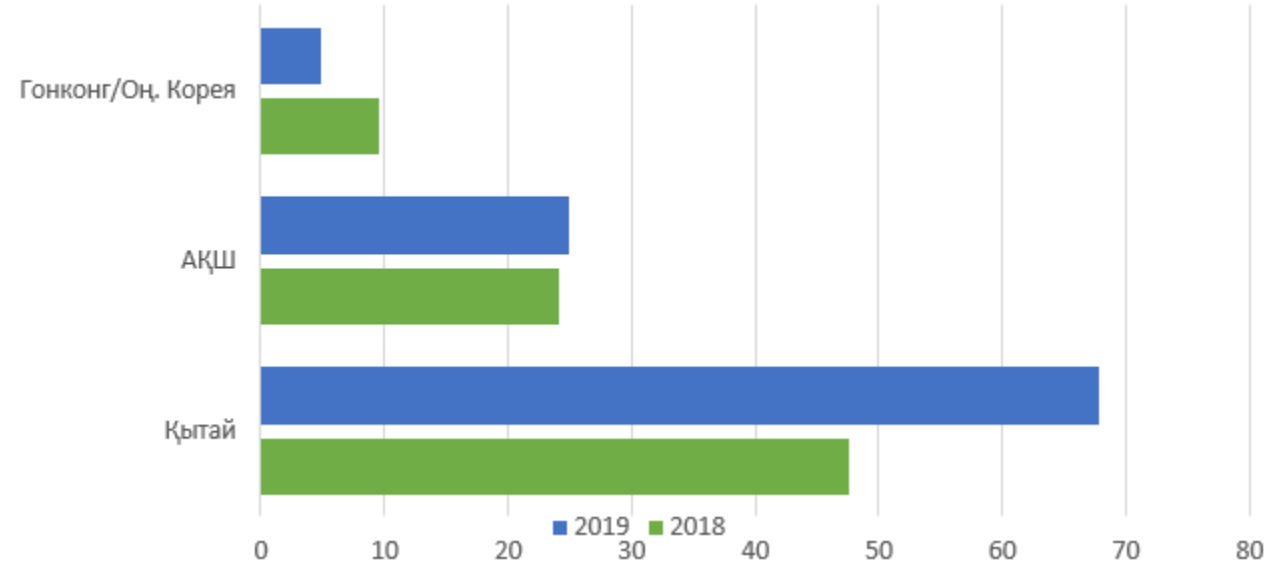


1.5 сурет – Шабуылдар үлесі

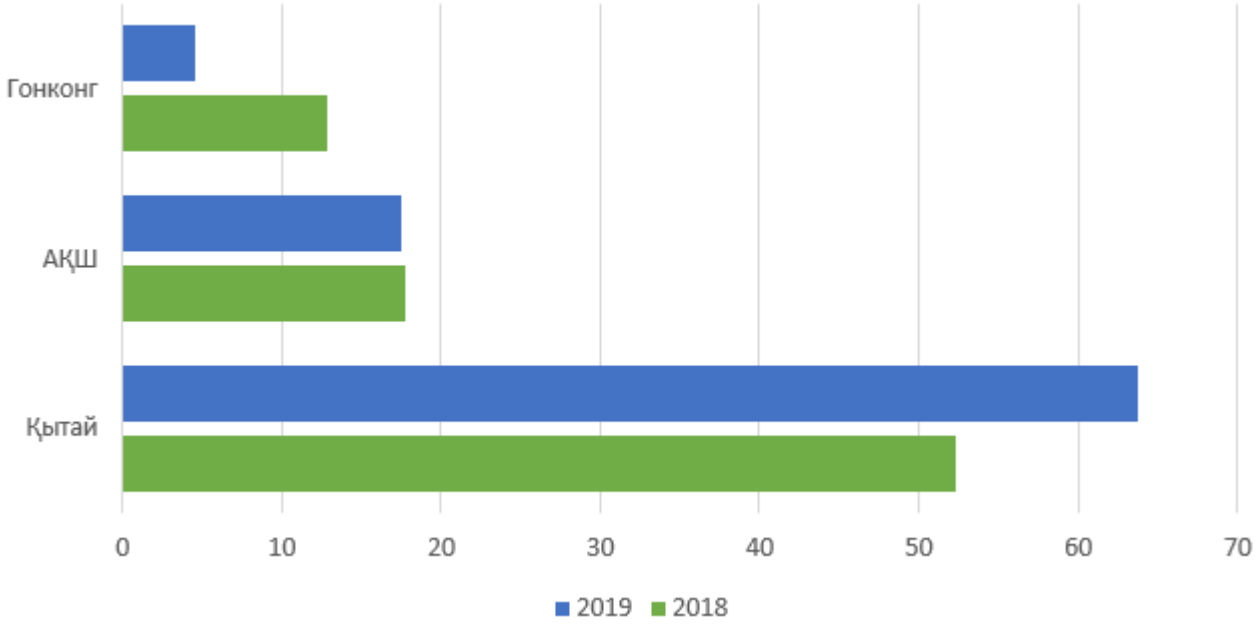
DDoS-шабуылдар

Бұлтта "қызмет көрсетуден бас тарту" түріндегі шабуылдар қолданылуы мүмкін, олар инфрақұрылымның шамадан тыс жүктелуін тудырады, бұл жүйе ресурстарының үлкен көлемін іске қосуға мәжбүрлейді және тапсырыс берушілерге осы қызметті пайдалануға бере алмайды. Баспасөздің назары көбінесе бөлінген немесе DDoS-шабуылдарды тартады, бірақ бұлттық

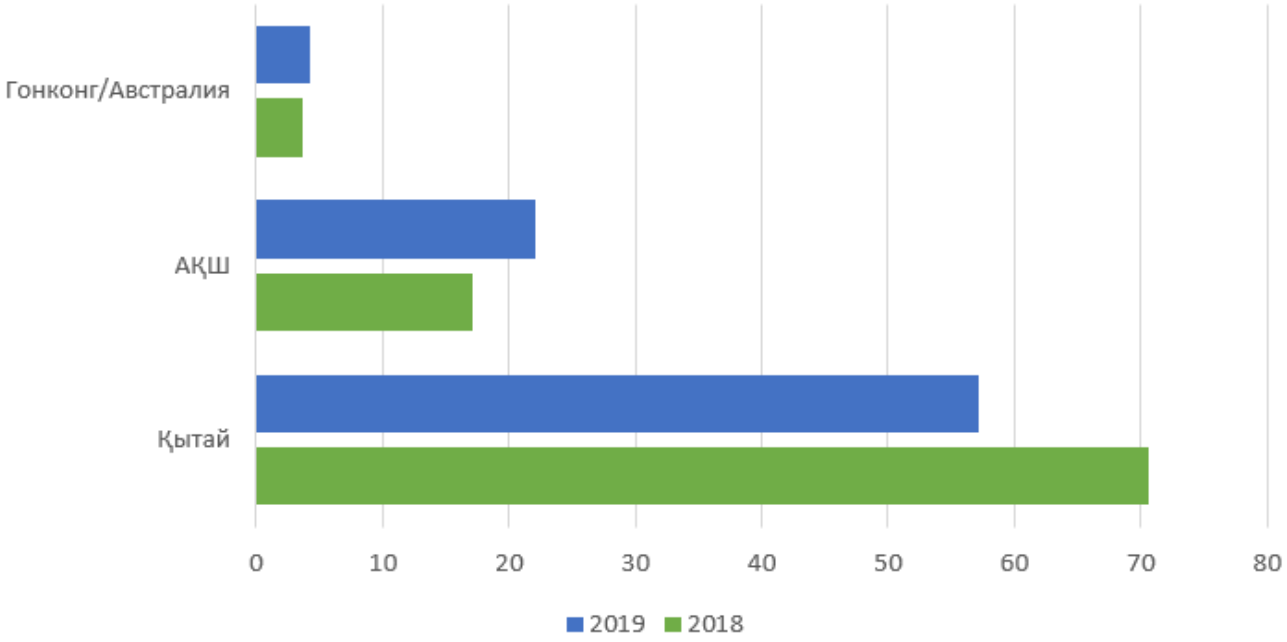
есептеулерді бұғаттай алатын DoS-шабуылдардың басқа да түрлері бар. Мысалы, зиянкестер Web-серверлердегі, деректер базаларындағы немесе басқа да бұлтты ресурстардағы осалдықтарды пайдалана отырып, өте аз пайдалы жүктememен қосымшаны құлату үшін қолданбалы деңгейдегі асимметриялық DoS-шабуылдарды іске асыра алады.



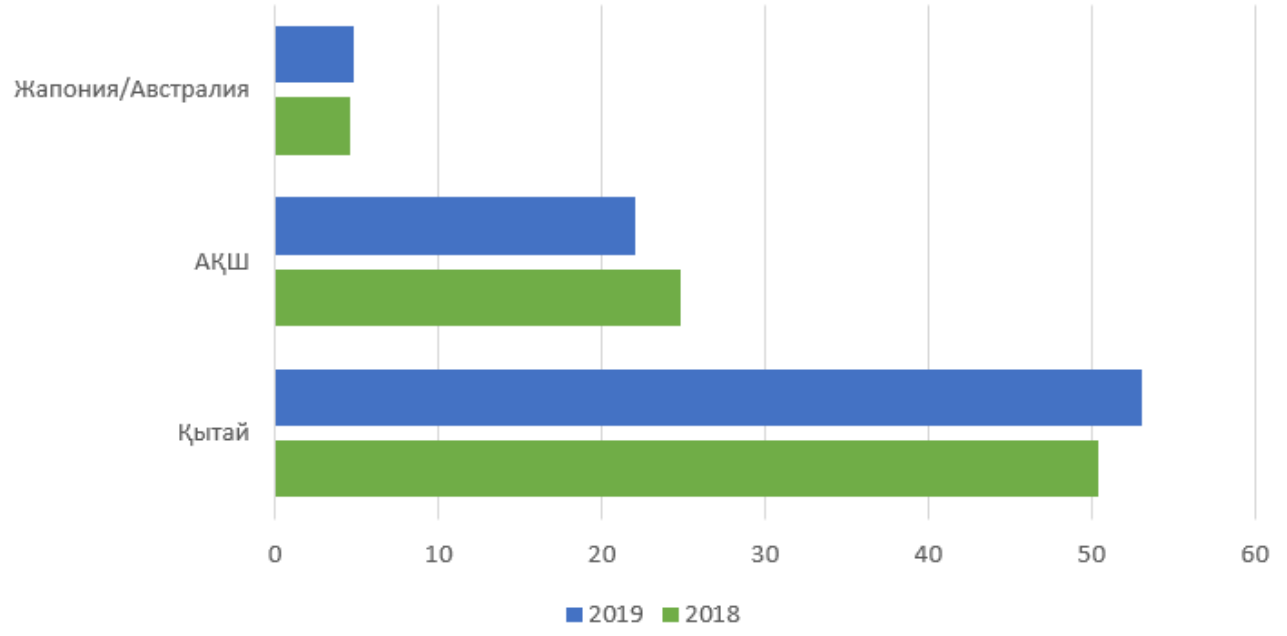
1.6 сурет – 1-ширектегі шабуылдар үлесі



1.7 сурет – 2-ширектегі шабуылдар үлесі



1.8 сурет – 3-ширектегі шабуылдар үлесі



1.10 сурет – 4-ширектегі шабуылдар үлесі

2019 жылдың қорытындысы бойынша әлемдегі DDoS-шабуылдардың саны 2018 жылға қарағанда 180%-ға өсті, ақпараттық қауіпсіздікті қамтамасыз ету технологияларына маманданған Neustar компаниясында есептелді.

2019 жылы ең күшті шабуыл 587 Гбит/с қуаттылығына ие болды, бұл өткен жылдың ең жоғарғы көрсеткішінен 31% - ға артық. 2019 жылы DDoS-

шабуылдың шекті қарқындылығы секундына 343 млн пакет өлшенді — бұл бір жыл бұрын 252% - ға артық.

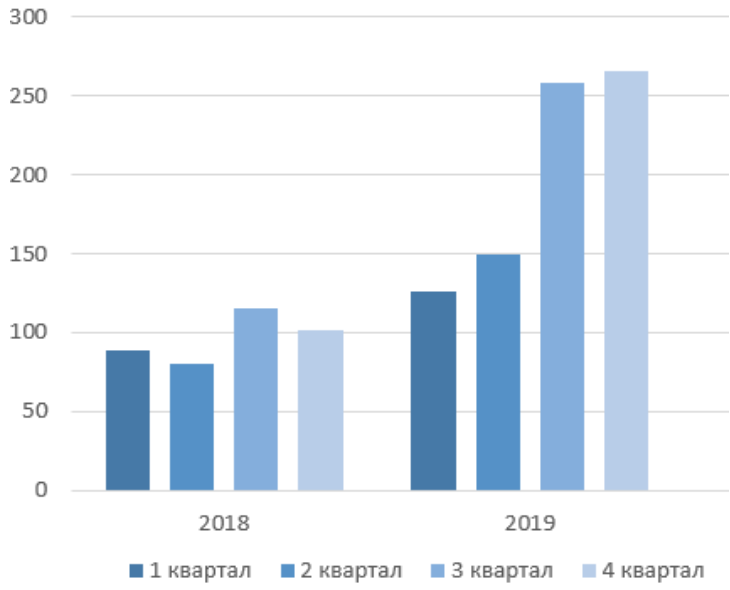
Сондай-ақ, сарапшылар өте тәжірибелі киберқылмыскерлер жүзеге асыратын ақылды DDoS-шабуылдар мен желілік инфрақұрылымға тікелей бағытталған шабуылдар санының өсуін атап өтті.

2019 жылы барлық шабуылдардың шамамен 85% - ы қауіптердің кемінде екі бағытын пайдаланды. Бұл сан 2018 жылғы көрсеткішпен салыстырылады; алайда екі немесе үш векторды пайдалану арқылы шабуылдар саны 55% - дан 70% - ға дейін өсті, тиісінше қарапайым бір бағытты шабуылдар мен күрделі төрт және бес бығытты шабуылдар саны азайды.

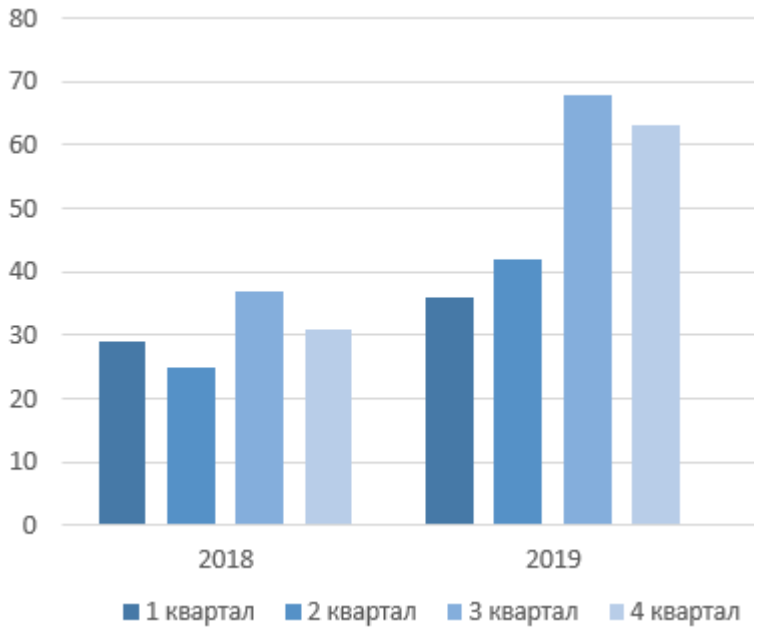
Neustar - да сондай-ақ ақпараттық қауіпсіздік мамандарынан сұрау барысында, олардың 58%-ы электрондық поштаны және бопсалаушы вирустарды пайдалана отырып, әлеуметтік инженериямен қатар киберқауіпсіздердің өсіп келе жатқан бағыт түрін DDoS-шабуылдарын атап өтті.

Әлеуметтік инженерия

Әлеуметтік инженерия — бұл адамдардың ойлары мен іс-әрекеттерін манипуляциялау әдісі. Ол тұлғаның психологиялық ерекшеліктері мен адам ойлауының заңдылықтарына негізделеді. Кейде құпия деректерге рұқсатсыз қол жеткізу әдісі ретінде әлеуметтік инженерияның түсінігін кездестіруге болады, бұл шындыққа сәйкес келмейді: бірқатар психологиялық әсер ету техникалары заңды түрде қолданылуы мүмкін. Дегенмен, қазіргі таңда құнды жабық ақпаратты алу әлеуметтік инжинирингті қолданудың негізгі салаларының бірі болып табылады.



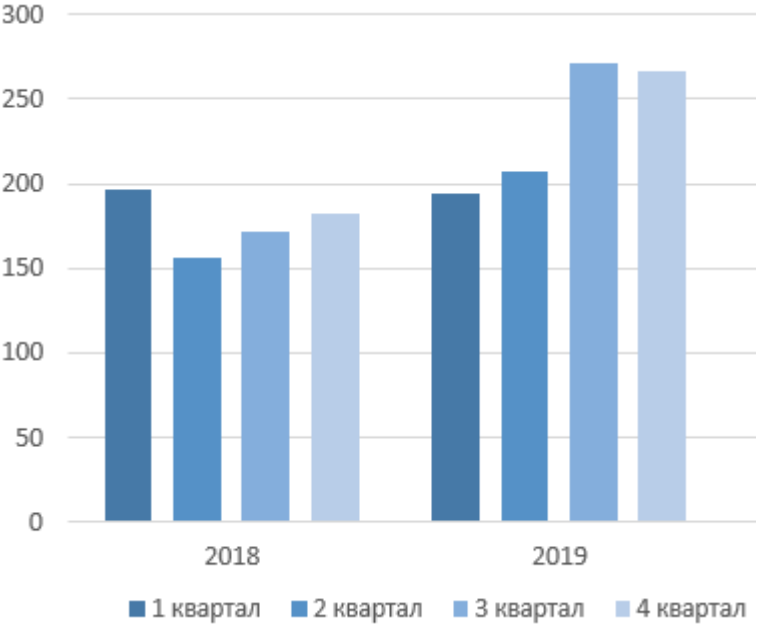
1.11 сурет – Шабуылдар саны



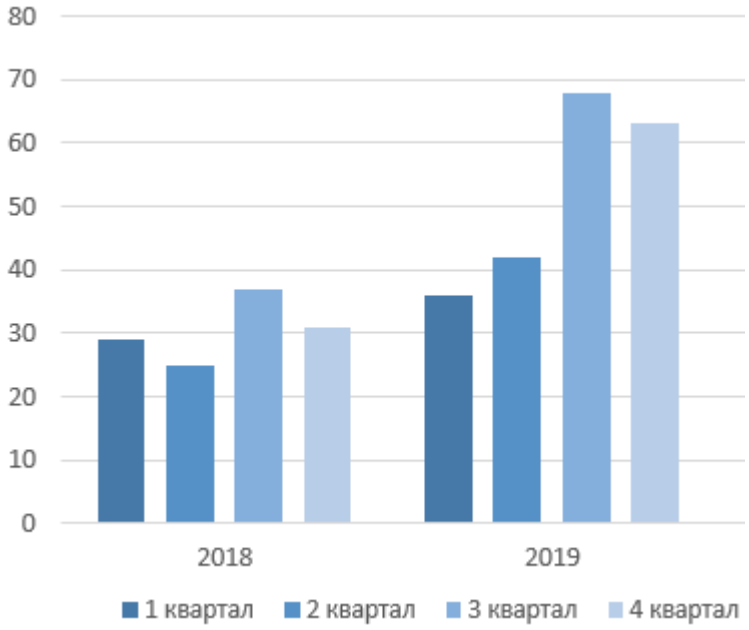
1.12 сурет – Шабуылдар үлесі

Зиянды бағдарлама

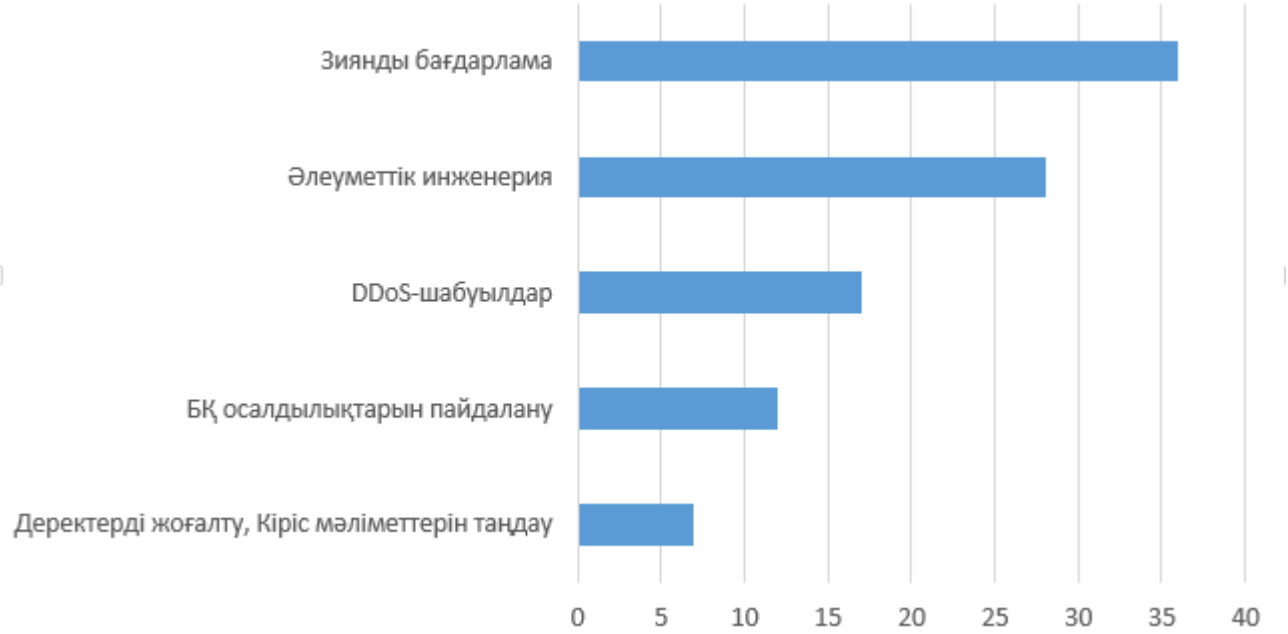
Зиянды бағдарлама — сервер (немесе ДК) ресурстарын рұқсатсыз пайдалану немесе ақпарат иесіне сервер (немесе ДК) желісінің иесіне ақпаратты көшіру, бұрмалау, жою немесе ауыстыру жолымен зиян келтіру (залал келтіру) мақсатында сервердің (немесе ДК) өзінің есептеу ресурстарына немесе серверде (немесе ДК) сақталатын ақпаратқа рұқсатсыз қол жеткізуге арналған кез келген бағдарламалық қамтамасыз ету.



1.13 сурет – Шабуылдар үлесі



1.14 сурет – Шабуылдар үлесі



1.15 сурет – Қортынды шабуылдар үлесі

Қортындылай келе шабулдардың жалпы үлестен қанша пайыз алатынын көріп отырмыз. Осы статистикалық мәліметтер негізінде шабулдың көп бөлігі зиянды бағдарламалар арқылы жүзеге асырылатын және осымен қоса әлеуметті инженерия екеу қатарлас екендігін байқадық. Бұның бірден-бір себебі әлуметтік инженерия арқылы зиянды бағдарламаларды қолданушы серверлеріне немес бұлттық сервистерін жұқтырып сол арқылы ақпаратқа қол жеткізеді. Зиянды бағдарламалар дамуына жаңа толқын алып келген шифрлаушы бағдарламалар

болып табылады және әлуметтік инженериямен тығыз қолданысқа ие. Мысалы, киберқылмыскер жалған хат арқылы немесе өзін басқа адамға беру арқылы зиянды бағдарламаны іске қостыртуы мүмкін кейінен ол бағдарлама ақпарат жоғалуына себеп болуы мүмкін.

DDoS - шабуылдарына келсек бұл шабуыл түрі жылдан жылға дамуда және киберқылмыскердің тәжірбиесі негізінде «Ақылды» DDoS шабулы пайда болып отыр. Бұл шабуыл ұйымдастыру жағынан өте күрделі және киберқылмыскерден өте көп тәжірбие талап етеді. Статистикалық мәліметтерге қарасақ шабулдар жасалатын аймақ Қытай, АҚШ, Гонконг жерлерінен жасалады және 2018 жылмен салыстырғанда 2019 жылы Қытай аймақтаынан жасалатын шабуылдар санының өсуін көреміз. Ал, АҚШ пен Гонконг шамамен бір келкі жағдайды екендігін байқаймыз. Қәзіргі, жағдайда бұл шабуыл түрі алдыңғы шабуылдардан күрделі болғанымен танымалдылығымен бұлттық сервистерге әкелетін зардаптары өте ауыр.

Бағдарламалық қамтама осалдықтарын пайдалану арқылы жасалатын шабуылдар тек тәжірбиелі мамандар қолынан келеді және маманның бағдарламаны зерттеуге өте көп уақытын алады. Тағы күрделендіретін жайт қәзіргі заманда жаңартулар ай сайын немесе оданда жиі келуі мүмкін сол себепті бағдарламалар мүмкіндігінше қауіпсіз болып саналады. Бірақ кей жағдайларда ескі немесе қолдау уақыты біткен бағдарламаларда көп ақаулар табылып жатады және ол ақауларды ешкім түземейді сол жағдайларға байланысты ақпарттар ұрланады немесе жайылады.

Деректерді жоғалту және кіріс мәліметтерін таңдау өте аз жағдайда жүзеге асатын жайыттар болып табылады. Бұның бірден бір себебі қорғаныс жүйесін ұйымдастыру барысында бастапқыда талқыланатын жағдайлар болып саналады. Бірақ табиғи немесе басқада төтенше жағдайды болжау мүмкін емес.

1.5 Бұлтты қорғау шаралары

2019 жылы көбінесе бұлттты қоймаларынан ақпаратты зиянды бағдарлама көмегімен, кіріу мәліметтерін таңдау арқылы немесе қызметтің дұрыс емес баптауларындағы осалдылқтарды пайдалану арқылы ақпарттар ұрланды. Егер провайдер қарапайым ақпараттың қауіпсіздік шараларын жасаса, көптеген мәселелерді болдырмауға болады. Бұлтты ортаны қорғау үшін негізгі компаненттері:

– Брандмауэр, басып кіруді болдырмау құралы, антивирус және анти-бот (рұқсатсыз қол жеткізуге тыйым салуды және зиянды бағдарламалардан қорғауды қамтамасыз етеді).

– Қосымшаларды бақылау (бұлтты сервистер деңгейінде шабуылдарды болдырмайды).

– IPsec VPN (бұлт ресурстарына қауіпсіз қосылу орнатады).

– Екі факторлы аутентификация және құрылғыларды жұптастыру арқылы бұлтқа қатынауды бақылау құралы.

– Деректерді жоғалтудан қорғау жүйесі (құпия мәліметтерді ұрлаудан немесе абайсыздан жоғалудан қорғауды қамтамасыз етеді).

– Sandboxa (зиянды бағдарламалар мен нөлдік күннің шабуылдарынан белсенді қорғайды).

Бұл компоннеттер негізі болып есептеледі және әр компания өзіне керекті қорғаныс компоненттерін алумен ғана шектелуі мүмкін немес басқа компаниялардан дайын қорғаныс шешімдерін ала алады. Мысалы, McAfee компаниясы ұсынатын дайын шешімдер бар оның ішіне барлық жоғарыда келтірілген компненттер кіреді және сонымен қоса Office 365, Amazon Web Services (AWS) және Microsoft Azure қызметтеріне нормативтік-құқықтық сәйкестік пен қауіпсіздік талаптарын сақтау арқылы ауысға мүмкіндік береді. Бұнадай шешіммен отандық АО «Kaspi Bank» компаниясында кеңінен қолданысқа ие. Бұдан басқа CloudGuard компаниясына туындысы "бесінші буын" қауіп-қатерінлерінен қорғануға мүмкіндік береді. Виртуальды инфрақұрылым үшін Check Point CloudGuard IaaS қауіпсіздік саясатын орталықтандырылған басқаруды, оқиғалар журналын жүргізуді, мониторингті, оқиғаларды талдауды және есептеме жасауды қамтамасыз етеді. Сондай-ақ, ол трафикті ашық қайта бағыттау үшін SDN(Software-defined Networking) бақылаушыларымен интеграцияланған қызмет ретінде жеткізіледі. Ашық және жеке бұлттарға қойылатын талаптары 1.3, 1.4 – кестелерінде көрсетілген. Бұдан бөлек бұлтты брандмауэрлер кішкентай компанияларда үлкен сұранысқа ие. Себебі, көп қаражат және қосымша құрал жабдықтады талап етпиді дегенімен, қорғаныс жүйесін айталықтай жоғарылатады.

1.3 кесте – Ашық бұлтты инфрақұрылым үшін Check Point CloudGuard IaaS жүйелік талаптары.

№	Платформа	Қолдау көрсетілетін платформа нұсқалары
1	AWS	Amazon VPC
2	Google Cloud Platform	Google Cloud Platform
3	Microsoft Azure	Microsoft Azure Microsoft Azure Stack
4	Oracle Cloud	Oracle Cloud
5	Alibaba Cloud	Alibaba Cloud
6	IBM Cloud	IBM Cloud

1.4 кесте – Жеке бұлтты инфрақұрылым үшін Check Point CloudGuard IaaS жүйелік талаптары.

№	Виртуальизациа жасау платформасы	Виртуальдау платформасының қолдау көрсетілетін нұсқалары
1	VMware ESXi	vSphere 5 және кейінгі нұсқалары

2	Microsoft Hyper-V	2012 R2 Windows Server 2016 Windows Server
3	KVM	CentOS 7 RHEL 7
4	Cisco	APIC Version 1.3 / 2.0 / 2.1 / 2.2 / 2.3
5	VMware NSX	VMware vSphere 5.5 және кейінгі нұсқалары VMware vCenter Server 5.5 және кейінгі нұсқалары
6	Open Stack	Newton Ocata Pike

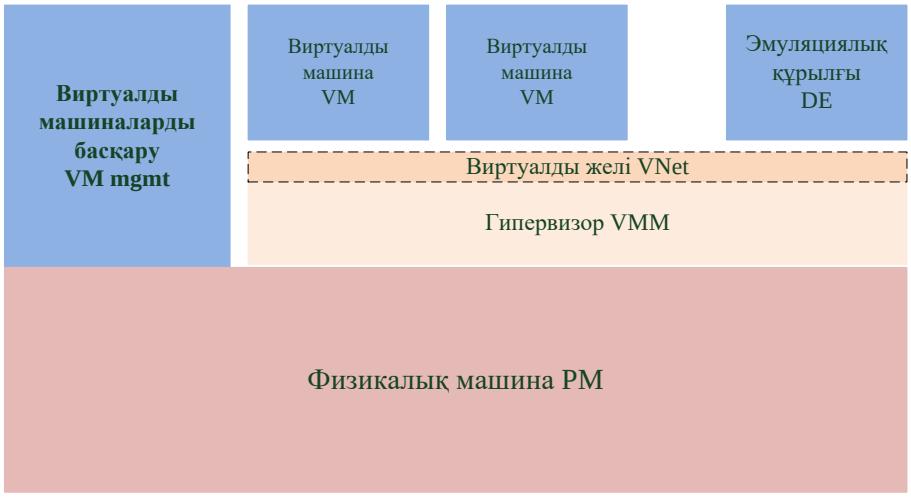
Брандмауэр

Web Application Firewalls (WAF) ретінде белгілі бұлтты брандмауэрлер сақиналы қорғау және бизнес-желілерді бөгде өндірушілердің зиянды шабуылдарынан қорғау тәсілі ретінде АТ қауіпсіздігінің үйреншікті бөлігі болып табылады. Бұл шабуылдар әртүрлі - "қызмет көрсетуден бас тарту" (DDoS) түріндегі таратылған шабуылдардан тікелей хакерлік шабуылдарға, зиянды бағдарламалық қамтамасыз етудің енуіне және сүзілуіне дейін түрленуі мүмкін.

Үздік бұлтты WAF брандмауэры Cloudflare WAF болып есептеледі. Себебі, бұлтта веб-қосымшаларды SQL-инъекцияларды қолдану арқылы жасалған шабуылдардан, сайтаралық скриптинг және сайтаралық қолданыстар сияқты кең таралған осалдықтардан, қолданыстағы инфрақұрылымдағы өзгерістерсіз қорғайды. Салыстырмалы түрде қызмет көрсету бағалары арзан және шағын компаниялар үшін өте тиімді. Компания пайдаланатын өзіне-өзі қызмет көрсету моделі қолданушыларға шеберлердің көмегімен баптауларды жылдам және оңай реттеуге мүмкіндік береді. Сондықтан клиенттер қызмет көрсетудің қарапайымдылығын жоғары бағалайды.

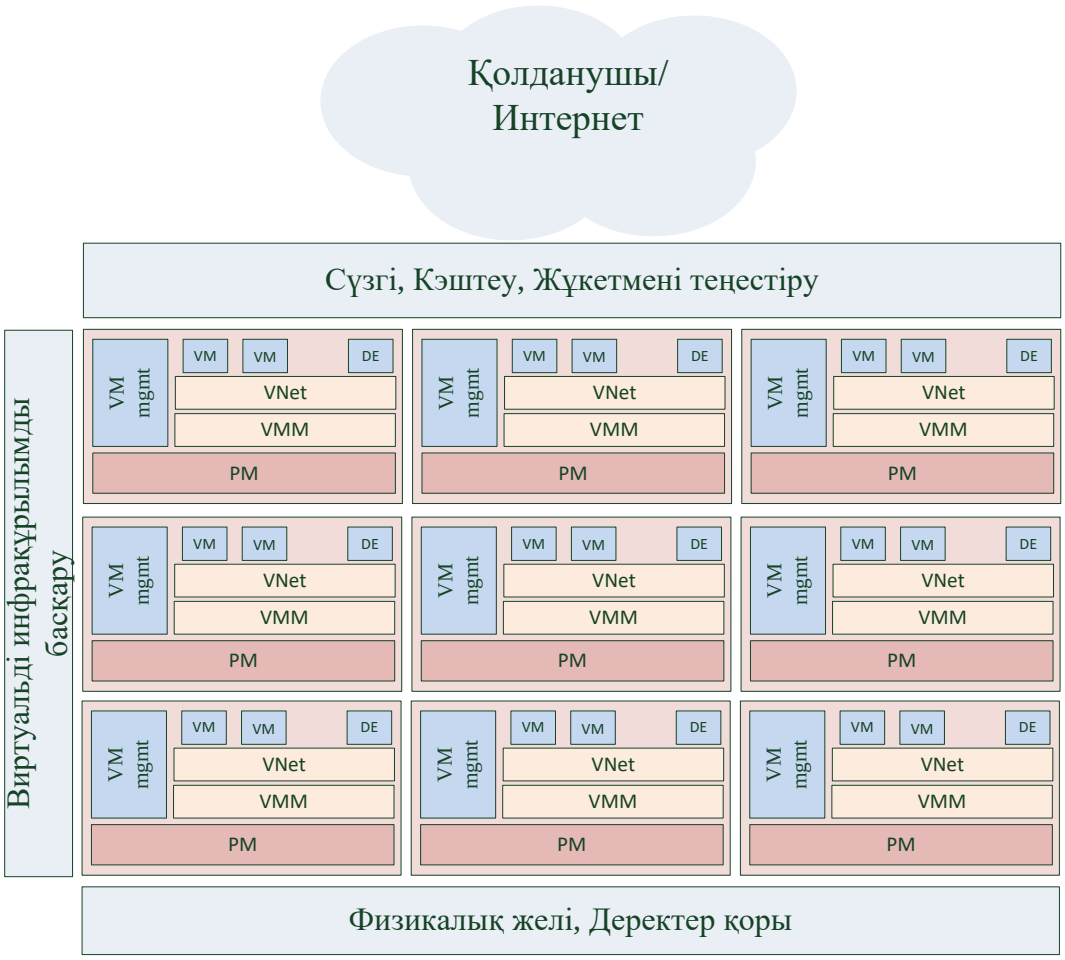
2 IaaS сервистік моделі

Виртуальдату сәултті құру кезінде динамикалық масштабталуға мүмкіндіктер береді. Масштабтауға қосымша, виртуалдату виртуальді машиналарды жүктеуді теңдестіру үшін бір физикалық серверден екіншісіне тасымалдауға мүмкіндік береді. сурет 2.1 көрсетілгендей виртуальді компонент гипервизор немесе виртуальді машиналардың мониторы (VMM) деп аталатын бағдарламалық қамтамасыз ету қабаты арқылы іске асырылады. Бұл қабат бірнеше операциялық жүйелерді және олардың қосымшаларын бір физикалық машинада бір мезгілде орындауға мүмкіндік береді. Гипервизордың үстінде операциялық жүйені, қосымшаларды және баптауларды қамтитын Виртуальді машина деп аталатын объект орналасқан. Егер қажет болса, онда гипервизорда немесе виртуальді машинада құрылғылардың эмуляциясы іске асырылуы мүмкін. Мұндай жүйені басқару үшін арнайы басқару сұлбалары қажет, онда виртуализацияның динамикалық табиғаты және ол ұсынатын жаңа мүмкіндіктер ескеріледі. Мұндай басқару жүйесі қабаттар түрінде жақсы іске асырылады, жергілікті басқаруды серверде жүзеге асыру, ал инфрақұрылымды басқаруды бүкіл виртуальді ортаны басқаруға арналған неғұрлым жоғары деңгейде орындау.



2.1 сурет – Бұлт жүйесіндегі негізгі түйін элементтері

сурет 2.2 көрсетілгендей көптеген түйіндер бірлесіп пайдаланылатын жады бар желілер арасында бөлінген және ортақ инфрақұрылымдық басқару, шығысында (front-end) интерфейсімен қоса жүктеуді теңестіру, кэштеу, сүзу (фильтрлеу) мүмкіндігін алады және осының бәрі виртуальді инфрақұрлымды құрайды немесе бұлт, бұлтты жүйені береді. Онда қолданылмайтын қуатты резервтеудің орнына қосымша есептеу қуаты сұралғанға дейін әрекетсіз машиналарды өшіруге болады. Тораптарда виртуальді машиналарды (статикалық немесе динамикалық) олардың жеке жүктелуіне байланысты теңдестіруді жүзеге асыруға болады.

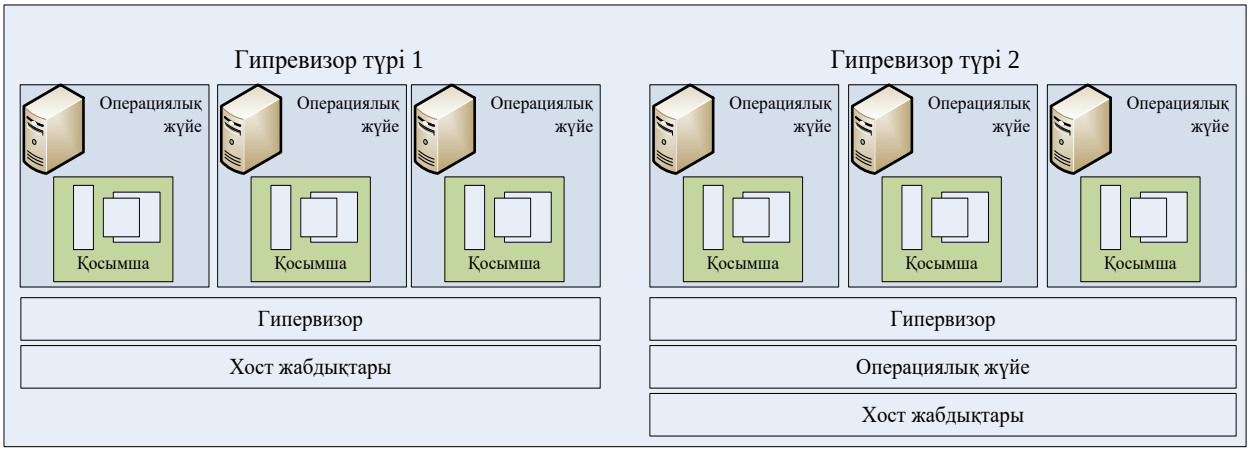


2.2 сурет – Бұлтты жүйенің есептеу инфрақұрылымы

Келесі бөлімде физикалық серверлерде тікелей жұмыс істейтін қолданыстағы гипервизор және бағдарламалық қамтамасыз етуді толық қамды қарастырамыз.

2.1 Гипервизор

Бұлттық жүйенің негізгі жүйелік ресурстарды виртуалдауға мүмкіндік беретін гипервизор - бағдарламалық немесе микро бағдарламалық қамтамасыз ету болып табылады. Гипервизор екі түрі бар. сурет 2.3 екі типті гипервизорлардың айырмашылықтары көрсетілген.



2.3 сурет – 1-ші түр және 2-ші түр гипервизорлар арасындағы айырмашылықтар

Гипервизор 1-ші түрі жүйе жабдықтарында тікелей жұмыс істейді. Гипервизор 2-ші енгізу / шығару және жадты басқару құрылғыларын қолдау сияқты виртуалдау қызметтерін қамтамасыз ететін базалық операциялық жүйенің үстінен жұмыс істейді.

Ең кең қолданылатын гипервизорды және олар қолдайтын аппараттық платформаларды қарастырайық:

– PowerVM: IBM POWER5, POWER6 және POWER7 негізіндегі серверлерге тиесілі, бұл гипервизор IBM i, AIX және Linux операциялық жүйелерімен қолдау көрсетеді; PowerVM SmartCloud Enterprise ортасында қолдау көрсетеді.

– VMware VSphere: кірістірілген гипервизор, қосымша амалдық жүйені талап етпей серверлер аппаратурасында тікелей жұмыс істейді. Ол өз VMware виртуалдау ортасында да, басқа әзірлеушілер ортасында да қолдау көрсетеді.

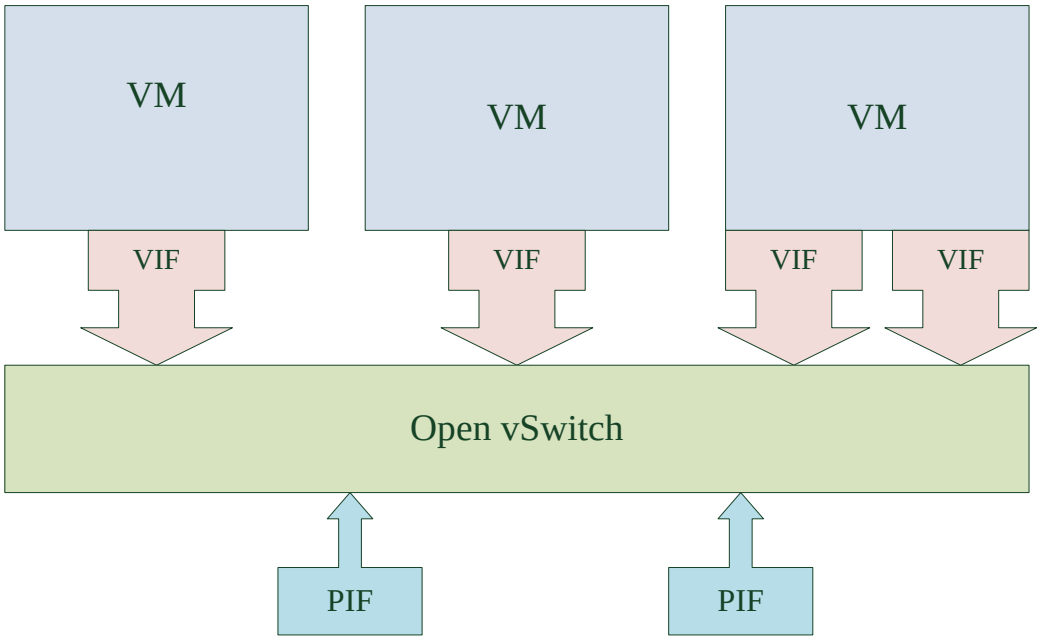
– Xen: IA-32, x86-64, Itanium және ARM, Xen процессорлық сәултті үшін виртуальді машиналар мониторы бір уақытта бір жабдықта бірнеше қонақтық операциялық жүйелерді орындауға мүмкіндік береді. Xen жүйелері XEN гипервизоры ең төмен және артықшылықты деңгейге ие құрылымға ие.

– KVM: Linux ядросы үшін виртуалдау инфрақұрылымы, KVM виртуалдандыру үшін аппараттық кеңейтімдері бар процессорларда базалық тәуелді виртуалдандыруды қолдайды. Бірінші кезекте ол x86 процессорларын қолдады, бірақ қазіргі уақытта оларға процессорлар мен қонақтық операциялық жүйелердің кең спектрі қосылды, оның ішінде Linux, BSD, Solaris, Windows ® , Haiku, ReactOS және AROS Research Operating System (QEMU өзгертілген нұсқасы бар, Mac OS X-мен жұмыс істеу үшін KVM қолдануға қабілетті) көптеген нұсқалары бар.

– z / VM: IBM, z / VM виртуальді машиналар операциялық жүйесінің ағымдағы нұсқасы IBM zSeries серверлерінде жұмыс істейді және Linux виртуальді машиналарының үлкен санын (мың) қолдау үшін пайдаланылуы мүмкін.

2.2 Виртуальді желі

Виртуальді машиналар физикалық серверлерде орналастырылады және олардың бір-бірімен және платформамен өзара әрекеттесуі үшін оларға желі қажет. Барлық виртуальді машиналарды физикалық деңгейде желімен біріктірудің орнына виртуальді машиналар арасындағы жергілікті өзара әрекеттесуді виртуалдандыру қолданылады. Виртуальді машиналардың өзара әрекеттесуін оңтайландыру үшін виртуальді коммутатор (virtual switch) қолданылады. Виртуальді коммутатор физикалық коммутатор ретінде жұмыс істейді (сурет 2.4). Бұл суретте виртуальді машиналар арасындағы өзара әрекеттестікте қолданылатын виртуальді интерфейстер (VIF) виртуальді коммутатор арқылы физикалық интерфейстермен (PIF) өзара әрекеттеседі.



2.4 сурет – Виртуальді және физикалық интерфейстермен vSwitch жалпы пайдалану сызбасы

Ашық код аумағында бұл мәселе Open vSwitch деп аталатын өнімнің және оның қарапайым ұқсас бағдарлама көмегімен шешіледі. Оның көмегімен виртуальді ортада виртуальді коммутатор іске асырылады, сондай-ақ физикалық платформалармен өзара әрекеттеседі және виртуальді жергілікті желілер (VLAN), сапа басымдылығымен қызмет көрсету (QoS), коммуникациялық топтық арналарды іске асыру, сондай-ақ аппараттық көп дәлдікті қолдау сияқты кәсіпорын деңгейінің мүмкіндіктері беріледі. Қазіргі уақытта Linux-та әртүрлі виртуальді шешімдерді (Xen, KBM, VirtualBox) қолдануға және әртүрлі басқару стандарттарын (Remote Switched Port Analyzer [RSPAN], NetFlow және т.б.) пайдалануға мүмкіндік беретін Open vSwitch нұсқасы қол жетімді.

2.3 IaaS сервитік моделін басқаруға арналған платформаларды салыстыру.

Провайдерлердің бұлтты сервистері дайын платформалардың базасында орналасқан. IaaS сервитік моделін басқаруға арналған кең таралған платформалардың мүмкіндіктеріне салыстыру.

2.3.1 Cloudstack платформасы

Cloudstack – жеке инфрақұрылымның есептеу ресурстарын басқару консолі. Бұл платформада Zynga, Nokia Research Center, Cloudcentral сияқты ірі компаниялардың инфрақұрылымы салынған. Жобаны дамыту Citrix компаниясының қолдауымен жүзеге асырылады. Платформа өз API бар, ол оны қолда бар инфрақұрылыммен теңшеуге және біріктіруге мүмкіндік береді, ал CloudBridge Amazon EC2 өтпелі жолы арқылы Amazon API-ді CLOUDSTACK API-ге алмастыруға болады.

Негізгі артықшылықтары:

– Әртүрлі гипервизорларды бір мезгілде қолдау (KVM, XEN, ESXi, OVM, BareMetal).

– Пайдаланушылар үшін рөлдер.

– Виртуальді желі.

– Ресурстар пулы.

– Күй суреттері ВМ (snapshots).

– Виртуальді маршрутизаторлар, ферволдар, жүктемені теңгеруші.

– Live Migration (жұмыс істеп тұрған ВМ қызмет көрсетуді үзбей орын аустыру(миграциялау)).

При ESXi гипервизормен жұмыс істеу үшін vCenter API платформасын пайдаланады. Бұл VMware-да салынған қолда бар инфрақұрылымға платформаны енгізуді айтарлықтай жеңілдетеді.

Қазір Cloudstack тегін және GNU Public License Version 3 лицензиясымен таратылады және ақылы қолдау жазылым нұсқасы бар. Платформаны орнату кезінде туындаған мәселелерді қоғамдастыққа ресми форумға хабарласу арқылы шешуге болады. Сондай-ақ, IRC арнасы бар, онда қалаған жауаптарды алуға болады.

Барлық өнімдердің маңызды бөлігі құжаттама болып табылады. Оның егжей-тегжейі мен қамтылуына пайдаланушының осы технологияға кіруінің жеңілдігі байланысты. Құжаттама оңай және түсінікті болған сайын, платформаны мүдделі тұлғаны теңшей алады. Белгілі бір тәжірибеге ие бола отырып, қарапайым платформаны инсталляциялау мүмкін, бұл танысу үшін жеткілікті.Сәулетті жоспарлау мен инсталляциялау қиынырақ уақытты алады, өйткені құжаттамада барлық ерекшеліктер ашылмайды. Ол step by step стилінде жасалған және платформа жұмысының ерекшеліктерін сипаттамайды. Білімнің

бір бөлігін белгілі бір уақыт ішінде платформаны нақты пайдаланғаннан кейін ғана алуға болады.

Cloudstack-кең функционалға ие инфрақұрылымды басқарудың тамаша консолі. Консоль тегін және жылдам қарқынмен дамуда. Оны қиындықсыз қолданыстағы инфрақұрылымға енгізуге болады, бірақ тек ESXi гипервизорларын ғана пайдаланған жағдайда, ең жақсы нұсқа vCloud Director пайдалануға болады.

2.3.2 Eucalyptus платформасы

Eucalyptus – бұлттарды құру үшін келесі қарастырылатын платформа. Бұл платформада Sony, Puma, NASA және Trend micro сияқты ірі компаниялар салынды. Eucalyptus екі редакцияда шығарылады, ақылы және тегін. Eucalyptus бар негізгі артықшылығы оның API-мен Amazon API-мен толық үйлесімділігі болып табылады. Amazon API-мен жұмыс істейтін барлық скрипттер мен бағдарламалар Eucalyptus платформасында салынған жеке бұлтқа ауыртпалықсыз көшірілуі мүмкін дегенді білдіреді. Жүйе 3 гипервизорды қолдайды: XEN, KVM, ESXi. Соңғы (ESXi) тек Enterprise нұсқасында қолдау көрсетеді.

Негізгі артықшылықтары:

– Пайдаланушылар үшін рөлдер.
– Әртүрлі гипервизорларды бір мезгілде қолдау.
– Кластерлер мен аймақтарға бөлу.
– Желіні басқару икемділігі, трафикті оқшаулау, қауіпсіздік топтары.

Өнім орнату бойынша құжаттамамен қамтамасыз етілген, бірақ ол жұмыстың барлық аспектілерін толық жабпайды. Жүйені орнататын адам айтарлықтай тәжірибесі бар деп болжанады. Құжаттама виртуализация параметрлерін немесе стандартты Схемадан айырмашылықты қамтымайды. Бұл күрделі конфигурацияны орнату кезінде тек өз тәжірбиесіне сүйену керек дегенді білдіреді. Eucalyptus тегін нұсқасы белсенді дамуда емес алайда, коммерциялық нұсқасы өте қарқынды дамуда.

2.3.3 vCloud Director платформасы

VCloud Director – VMware бұлттарды құруға арналған платформа. Егер барлық инфрақұрылым VMware өнімдерінде салынса, ең жақсы шешім vCloud Director енгізу болады. Бұл жүйе шын мәнінде гибридті бұлттарды құруға мүмкіндік береді. VMware vCloud Connector арқылы бұлттың көпшілік және жеке бөліктері арасында виртуальді машиналардың тасымалдануын жүзеге асыруға болады.

Негізгі артықшылықтары:

– Виртуальді датаценттер.

– VShield қауіпсіздігін қамтамасыз ету технологиялары.
– Инфрақұрылым қызметтерінің каталогы.
– Өзіне-өзі қызмет көрсету порталы.
– VMware vCloud API, Open Virtualization Format форматында виртуальді машиналар.

Платформа vCloud Director коммерциялық яғни, ол ақылы түрде жүзеге асырылады, барлық қолданушылар сатып алғаннан кейін толық қолдау алады. Қажетті пакеттің бағасы бойынша өңірлік өкілдерге жүгінуге болады. VMware нарық көшбасшысы болып табылады және үлкен қауымдастықты қалыптастыратын өте кең аудиторияға ие, үнемі қолдау қызметіне жүгінбей қиындықтарды шешуге көмектесетін білім базасын толықтырады.

2.3.4 Openstack платформасы

Openstack – ашық бастапқы коды бар бұлтты инфрақұрылымдарды құруға арналған платформа. Openstack жобасына 3 өнім кіреді: Nova (Amazon EC2 аналогы), Swift (Amazon S3 аналогы), Glance (бейнелерді ұсыну қызметі). Оның бірінші бөлігін қарастырайық. Қазіргі уақытта, Nova толық 2 гипервизор қолдайды: KVM және XEN. Платформа Cisco, Dell, NASA, Intel, AMD, Citrix, Rackspace, Rightscale сияқты корпорациялар тарапынан үлкен қоғамдастық пен қолдау ала отырып, тез дамып келеді. Openstack негізгі ядросы NASA әзірлеген Nebula өнімі болды.

Негізгі артықшылықтары:
– Виртуальді серверлер ресурстарын басқару.
– Виртуальді желілерді басқару.
– Виртуальді машиналардың кескіндерін басқару.
– Қауіпсіздік топтары.
– Рөлдерге негізделген кіруді бақылау.
– Жобалар мен квоталар.
– Веб браузерде VNC арналарын проксирлеу.

Өнім толығымен тегін, бастапқы ашық кодтармен. Openstack-те, осы бөлімде қарастырылған барлық платформалар, ең үлкен және белсенді қоғамдастық. Өнімнің белсенді дамуына байланысты, онымен қауымдастық деңгейінде шешілетін мәселелер жиі туындайды. Жылдам даму тек жаңартылып үлгермейтін құжаттамаларға да әсер етеді.

2.1 – кестеде осы бөлімде қарастырылған басқару жүйелерінің мүмкіндіктерін салыстыру келтірілген. Кестеде ең әмбебап және толық мүмкіндіктері тегін жүйе CloudStack болып табылады.

2.1 кесте – Инфрақұрылымды басқару жүйелерінің мүмкіндіктерін салыстыру

Мүмкіндіктері	Cloudstack	Eucalyptus	Openstack	vCloud Director

AD мен интеграция	+	-		+
Консоль басқару	+	Тек ақылы нұсқасында	+	+
ВМ консольне желі арқылы кіру	+	Тек KVM үшін	+	+
API	+	+	+	+
Multi–role	+	+	+	+
VLAN	+	+	+	+
Гипервизорлар	KVM, XEN, ESXi, OVM, BareMetal	KVM, XEN, ESXi (тек ақылы нұсқасында)	KVM, XEN	ESXi
Оңай шаблон жасау мүмкіндіктері	+	-	-	+
SnapShot	+	+	+	+
Дабыл және хабарламалар	+	-	-	+
Томдар (Volumes)	+	+	+	+
Қонақ ОЖ қолдау	Гипервизорді-кіндей	Linux	Гипервизорді-кіндей	Гипервизорді-кіндей
Live migration	+	-	-	+
Тегін	+	+/-	+	-
Amazon API мен үйлесімділігі	+	+	+	-
Rightscale	+	+	+	+
High Availability components	+	+	-	+
Енгізу	-	+	+	-

қиындығы				

2.4 Қазақстандық провайдерлер қызметтерінің салыстырмалы сипаттамасы

Қазақстанның "бұлтты" нарығы тек қана дами бастағандықтан, шетелдік провайдерлер сияқты қызметтердің алуан түрлілігін ұсына алмайды. Батыс провайдерлеріне ұқсас қызметтердің толық тізімі бойынша салыстыру жүргізу үшін жеткілікті ақпарат жеткіліксіз, өйткені отандық провайдерлер жалпы сипаттамаға жатпайтын қызметтерді ұсынады.

Бүгінгі таңда Қазақстан нарығында IaaS провайдерлері арасында үш ірі компаниялар бар олар «Қазақтелеком», «Ұлттық ақпараттық технологиялар», «Казтелепорт».

«Қазақтелеком» акционерлік қоғамы – бұлтты технологиялар даму және ауқымы бойынша Қазақстандағы монополист болып саналады. Бұндай артықшылықтар басқа кіші компанияларға кері әсерін бергенімен жалпы даму бойынша өте үлкен үлес қосуда.

«Ұлттық ақпараттық технологиялар» акционерлік қоғамы («ҰАТ» АҚ)– Қазақстан ақпараттық технологиялар нарығындағы ірі компания. Компания 2000 жылы Қазақстан Республикасы Үкіметі сәуірдің 4-і бекіткен «Қазақстан Республикасында бірыңғай ақпараттық кеңістіктің дамыту туралы» № 492 Қаулыға сәйкес құрылған. Қазіргі кезде «Қазақтелеком» АҚ кейінгі ірі компания болып саналады және Қазақстандық барлық электронды үкіметке байланысты проекттерді жүзеге асырады.

«Казтелепорт» акционерлік қоғамы – Қазақстандағы қарқынды дамушы команиялардың бірі. Қазтелепорт ерекшелігі басқа компанияларда жоқ немесе күрделі қызмет түрлерін ұсынуда және өзінің жұмыс қуатымен қоса нарыққа жаңа қызмет түрлерін ұсынуда.

Зерттеу барысында Қазақстандық ірі компаниялар Vmware бұлттарды құруға арналған платформа VCloud Director қолданатынын анықтадым. Себебі бұл платформа жеңіл орнатылады және гибридтті бұлттар құруға еркін мүмкіндік береді. VCloud Director платформасының тағы бірден-бір артықшылықтары оның VShield қауіпсіздігін қамтамасыз ету технологиялары және білім базасының үлкендігі. Енді осы үш компания ұсынатын қызметтеріне қарастырайық.

2.2 кесте – Отандық провайдерлердің қызмет түрлерін салыстыру.

Қызмет түрлері	Қазақтелеком	ҰАТ	Казтелепорт
Виртуальді дата-центр (IaaS)	+	+	+
Виртуальді серверлерді	-	-	+

репилкациялау (DraaS)			
Платформа қызмет ретінед (PaaS)	+	-	+
Бұлтты 1С	-	-	+
Резервті сақтау қызмет ретінде (BaaS)	+	-	+
Гибридті бұлт	+	-	+
Виртуальді бөлінген сервер (VDS,VPS)	+	+	+
Қаржылық есептілік қызметі (Finance Cloud)	-	-	+
Блокчейн	+	-	-
Бағдарламалық қамтамасыз етуді жалға беру	Microsoft Hosted SharePoint Microsoft Hosted Exchange Microsoft Hosted Lync	«Электрондық үкіметтің» ақпараттық-коммуникациялық платформасында орналастырылған бағдарламалық қамтама	Сұраным бойынша
Қауіпсіздік	DDoS шабуылынан қорғау Виртуальді Firewall	Байланыс арналарын криптографиялық шифірлеу арқылы қорғау	Security Operations Center (SOC) Ақпараттық қауіпсіздік қызметтері DDoS шабуылынан қорғау

Салыстырумызды қортындылай келе үш түрлі компания әр түрлі бағытта жұмыс жасайтынын анықтадық. Яғни, Казактелеком негізгі жұмысы виртуальді дата-центр қорын жалға беру болса, Ұлттық ақпараттық технологиялар көп қоры электронды үкіметке жұмсалады жәнеде қосымша виртуальді дата-центр жалға береді. Ал, Казтелепорт виртуальді дата-центрден басқа банктерге бағытталған қызметтер мен қауіпсіздікке көп көңіл бөлінген.

3 Жеке бұлт құру

Бұлт қоймасын пайдалану және кез келген уақытта интернет арқылы деректерге қол жеткізу мүмкіндігі өте ыңғайлы. Дегенмен, қауіпсіздікті қолдансаңыз, жеке және құпия деректерді бір жерде сақтау қауіпті екенін түсінуіңіз керек. Бұлттағы файлдарды шифрлау немесе жою мүмкін зиянды бағдарламалар бар. Сондай-ақ, пайдаланушылар өз деректерін кездейсоқ қайта жаза немесе жоя алады. Құпия ақпаратты алу мүмкіндігі оны заңсыз пайдалануға немесе сатуға мүдделі болуы мүмкін киберқылмыскерлерді тартады. Сол қауіптер бұлтты есептеулер негізінде ресурстарды пайдаланатын кәсіпорындарға таралады. Сондықтан бұлттарға төнетін қауіптерді толық қырастырып және соңғы статистикалық мәліметтерге шолу жасап қауіптің қаншалықты қатерлі екендігін бағалаймыз.

3.1 Жеке бұлт құру үшін қолданылатын бағдарламалар мен құрал-жабдықтар

Жеке бұлтта сервистер мен инфрақұрылымдық ресурстар жеке желі негізінде өзара байланысты. Мұндай модель қауіпсіздік пен бақылаудың анағұрлым жоғары деңгейіне кепілдік береді, бірақ бағдарламалық және аппараттық қамтамасыз ету шығындары комания сұранысына байланысты үлкен болуы мүмкін. Осындай жеке бұлт кемшіліктерін айналып өту үшін біз тегін OpenSource бағдарламаларын қолданамыз. Бұл шешім ірі компанияларға арналмаған тек шағын компания аумағында керекті құжат немесе деректер алмасуға аралған.

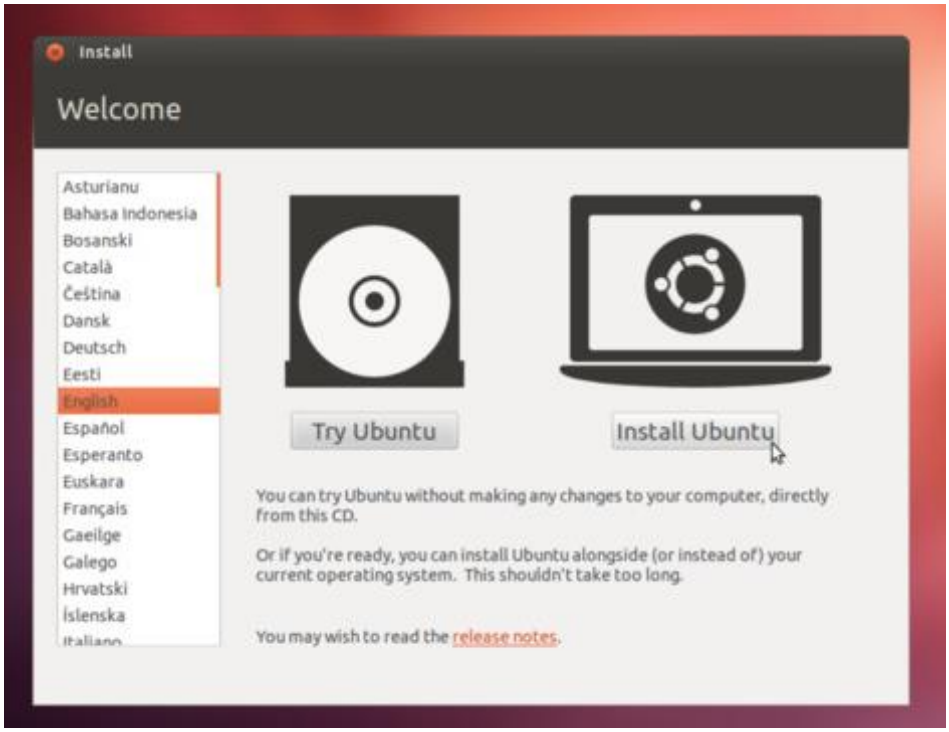
Бұлт құру үшін қажет бағдарламалар мен құрал-жабдықтар:

– Мини ДК MPC-0509X1900 (Сипаттамасы:CPU-Intel Celeron J1900, RAM-8gb, ROM-256gb)
– Ubuntu ОЖ
– Директориялады шифрлау
– NoMachine алыстан жұмыс жасауға арналған БҚ
– Apache HTTP веб-сервер
– MySQL деректер базасы
– Owncloud деректер алмасуға арналған БҚ
– SSL/TLS сертификаты

3.2 Жұмыс барысы

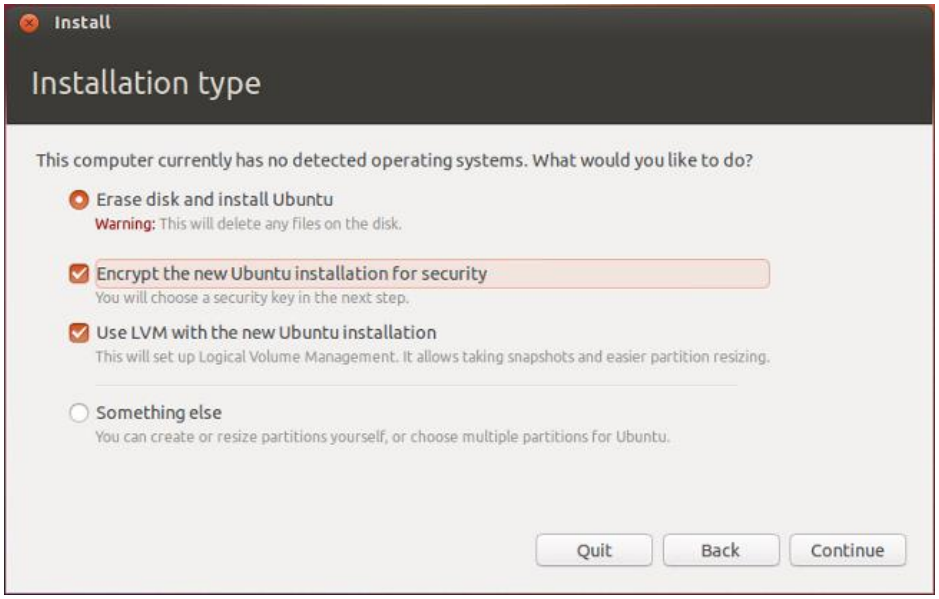
Қойылған мақсатқа қол жеткізу үшін біз ең алдымен негіз ретінде Ubuntu операциялық жүйесін орнатуымыз қажет. Орнату барысында деректерді шифрлау баптауын қосуымыз қажет бұл бізге қосымша қорғаныс береді. Келесі қадамымыз, NoMachine алыстан жұмыс жасауға арналған бағдарламаны орнату.

Бұл бағдарлама бір локальді желі ішінде тұрған компьтермен серверді басқаруға мүмкіндік береді және арасындағы байланыс NX шифрлау арқылы жүргізіледі. Кейіннен, біз Owncloud веб-бағдарламасын орнатамыз және баптауларына деректерді шифрлау, қолданушыларға құқықтар береміз және рұқсат етілген IP-мекенжайларын енгіземіз. Owncloud баптауларынан кейін Apache HTTP веб-сервер, MySQL деректер базасын Owncloud-қа енгіземіз және домен мен SSL/TLS сертификатының баптауларын реттеу арқылы жеке бұлтты интернет желісіне шығарамыз.



3.14 сурет – Ubuntu ОЖ орнату барысы

Орнату барысында деректерді қосымша қорғау үшін деректерді шифрлауды жүзеге асырамыз.

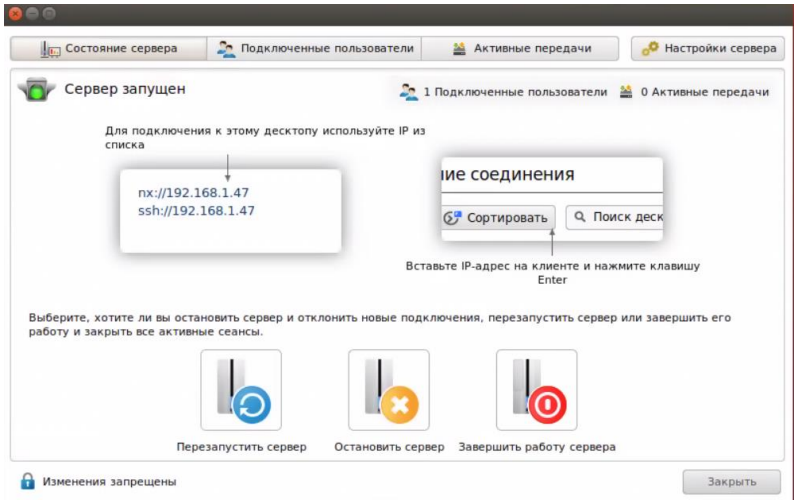


3.15 сурет – Деректерді шифрлау баптауын қосу

Операциялық жүйе орнатылғанна кейін қашықтан басқаруға арналған NOMACHINE бағдарламасын орнатамыз. Ол үшін консольге төменгідей командаларды енгізу қажет.

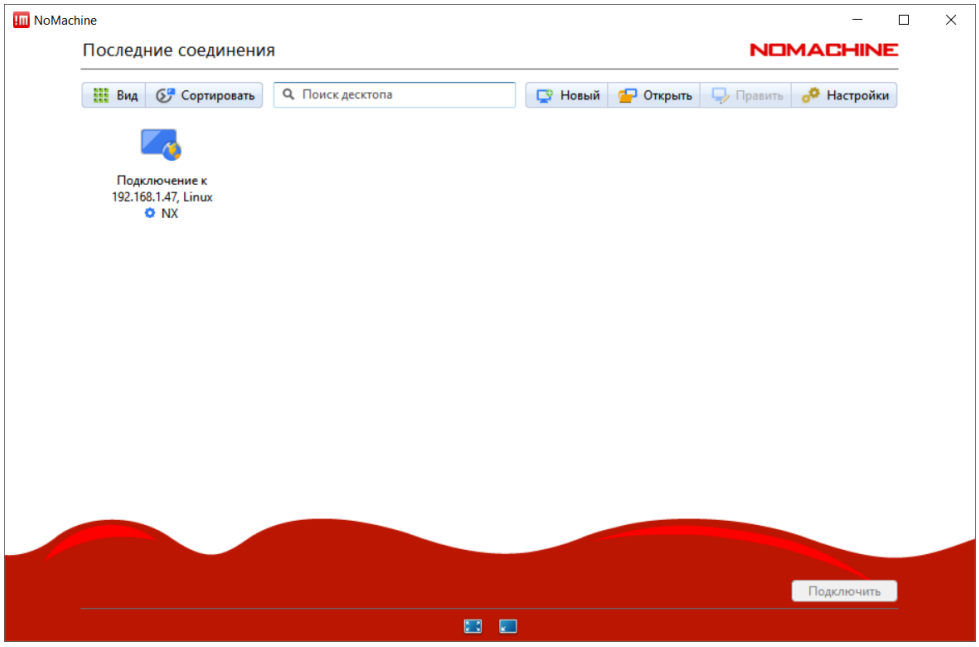
$wgethttp://download.nomachine.com/download/6.0/Linux/nomachine_6.0.78_1_amd64.deb

$sudo dpkg -i nomachine_6.0.78_1_amd64.deb

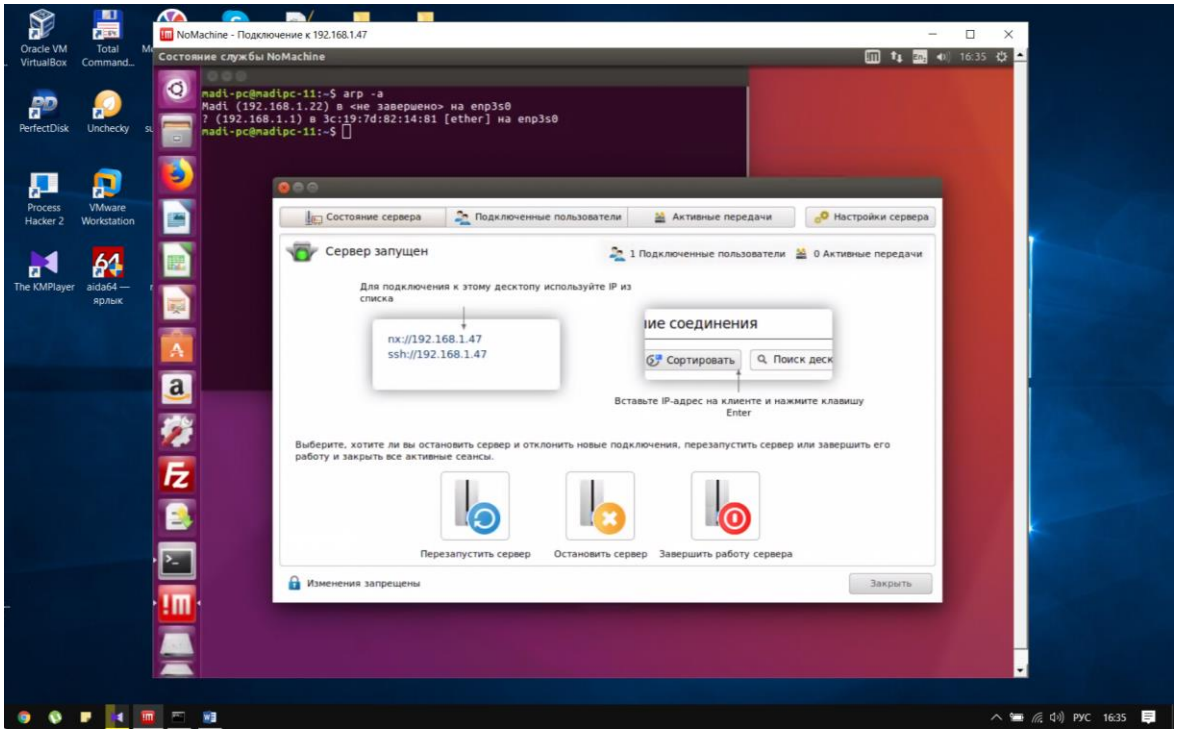


3.16 сурет – NOMACHINE бағдарламасы

Windows операциялық жүйеге nomachine.exe арқылы өзі орнатылады. Орнатылғанна кейін қашықтан серверге қосыламыз. Қосылуға мүмкіндігі бар компьтерлер бірден бастапқы интерфейсте көрсетіледі.



3.17 сурет – Қосылатын серверді таңдау



3.18 сурет – Серверге қашықтан қосылу

3.3 OwnCloud бағдарламасын орнату және іске қосу

OwnCloud бұл деректермен алмасу, файлдарға ортақ қатынасуға арналған еркін және ашық веб-бағдарлама. OwnCloud орнату үшін төмендегідей командаларды енгізу қажет.

#wget-q-Ohttps://download.owncloud.org/download/repositories/

stable/Ubuntu_16.04/Release.key | sudo apt-key add –

Apt-transport-https орнатылғанын тексереріуіміз қажет, өйткені біз келесі қадам үшін бұл бізге қажет болады:

```
# sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  aspell aspell-en dictionaries-common emacsen-common libaspell15
libexttextcat-2.0-0 libexttextcat-data liblua5.1-0 libyajl2
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 54 not upgraded.
Need to get 26.1 kB of archives.
After this operation, 215 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu xenial-updates/main amd64 apt-
transport-https amd64 1.2.26 [26.1 kB]
Fetched 26.1 kB in 0s (60.8 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 35616 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_1.2.26_amd64.deb ...
Unpacking apt-transport-https (1.2.26) ...
Setting up apt-transport-https (1.2.26) ...
```

Owncloud файлын құру қажет .list /etc/apt/sources.list.d себебі біз серверге OwnCloud репозиторий қосамыз

```
# echo 'deb https://download.owncloud.org/download/
repositories/stable/Ubuntu_16.04/ /' | sudo tee /etc/apt/sources.list.d/owncloud.list
deb https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04/ /:
```

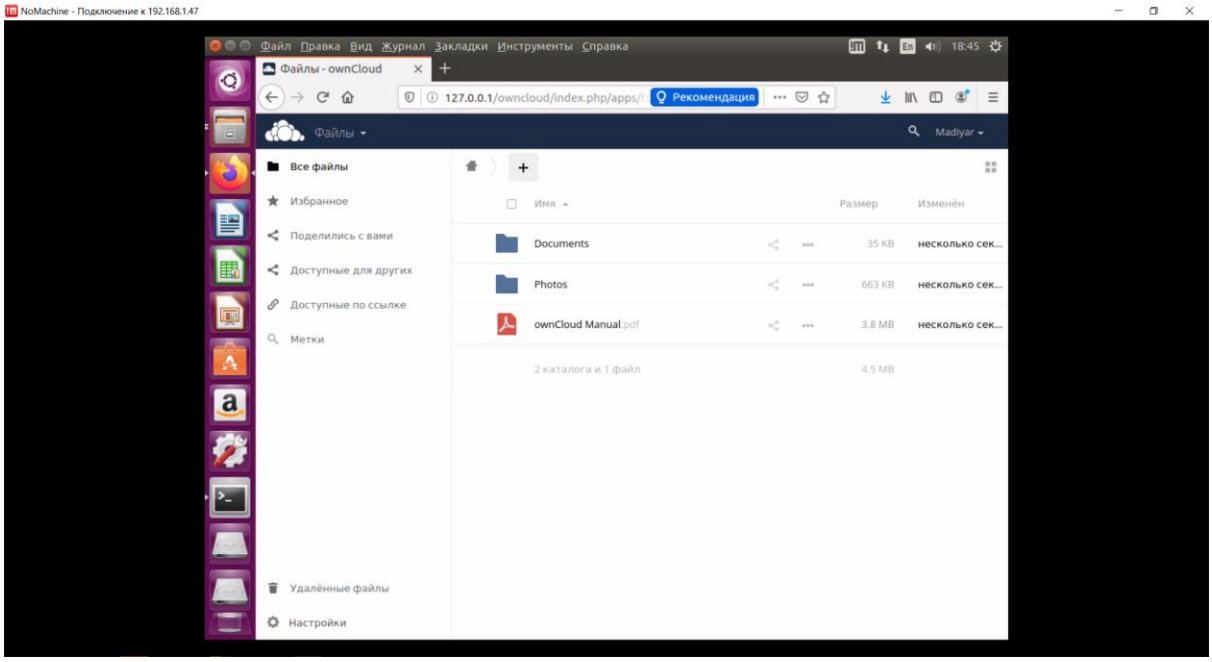
Енді біз OwnCloud пакеттерін орнату үшін жүйе пакеттерін қайта жаңартамыз:

```
# sudo apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://archive.ubuntu.com/ubuntu xenial-updates InRelease
Hit:3 http://archive.canonical.com/ubuntu xenial InRelease
Hit:4 http://security.ubuntu.com/ubuntu xenial-security InRelease
Ign:5 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04
InRelease
```

Get:6 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 Release [986 B]
Get:7 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 Release.gpg [481 B]
Get:8 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 Packages [736 B]
Fetched 2203 B in 2s (1030 B/s)
Reading package lists... Done

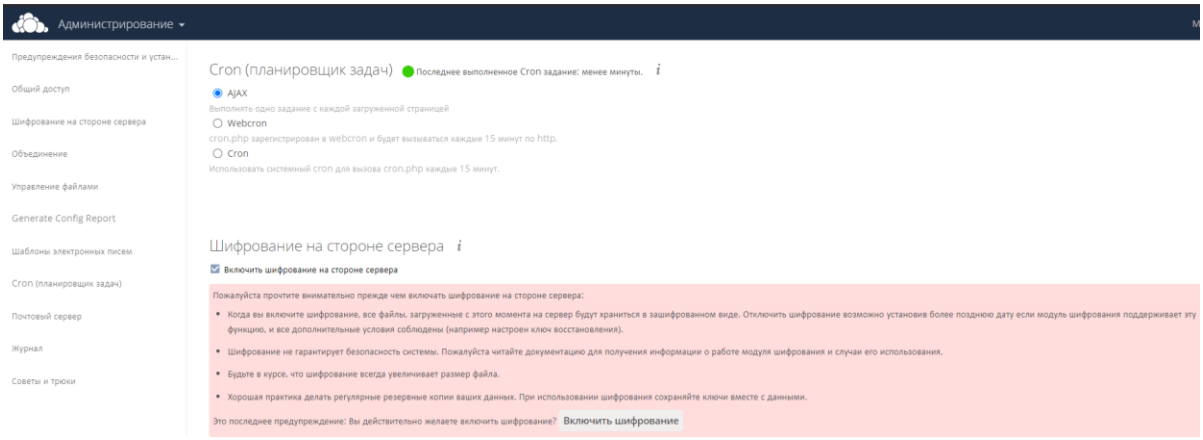
Төмендегі командаларды енгізе отырып OwnCloud орнату:

```
# sudo apt-get install owncloud-files
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  owncloud-files
0 upgraded, 1 newly installed, 0 to remove and 51 not upgraded.
Need to get 0 B/35.1 MB of archives.
After this operation, 118 MB of additional disk space will be used.
Selecting previously unselected package owncloud-files.
(Reading database ... 35869 files and directories currently installed.)
Preparing to unpack .../owncloud-files_10.0.7-1.1_all.deb ...
Unpacking owncloud-files (10.0.7-1.1) ...
Setting up owncloud-files (10.0.7-1.1) ...
```



3.19 сурет – OwnCloud бағдарламасы

Қосымша қорғаныс үшін OwnCloud баптаулар ішінен деректерді шифрлауды қосамыз.



3.20 сурет – Шифрлауды іске қосу

Енді келесі қадамымыз OwnCloud үшін MySQL деректер базасын жасау.

Root арқылы MySQL кіреміз:

mysql -u root –p

Енді біз келесі сұрау арқылы OwnCloud үшін MySQL деректер базасын жасаймыз:

mysql> CREATE DATABASE owncloud;

Содан кейін деректер базасымен өзара әрекеттесетін OwnCloud үшін жеке пайдаланушыны қосу үшін келесі сұрауды орындадық:

mysql> GRANT ALL PRIVILEGES ON owncloud.* to 'owncloud'@'localhost' IDENTIFIED BY 'enter_username_password_here';

Біз берген артықшылықтарды іске қосу үшін төмендегі команданы іске қостық:

mysql> FLUSH PRIVILEGES;

Енді біз MySQL сеансынан шыға аламыз:

mysql> exit;

OwnCloud-ты баптау

Алдымен, OwnCloud пакеттері дұрыс оранытылғанына көз жеткізіуміз тиіс:

sudo apt-get install libapache2-mod-php7.0 \

```
openssl php-imagick php7.0-common php7.0-curl php7.0-gd \
php7.0-imap php7.0-intl php7.0-json php7.0-ldap php7.0-mbstring \
php7.0-mcrypt php7.0-mysql php7.0-pgsql php-smbclient php-ssh2 \
php7.0-sqlite3 php7.0-xml php7.0-zip
```

OwnCloud сервері үшін Apache баптау

Енді біз ownCloud каталогына қызмет көрсету үшін Apache конфигурациясын баптауымыз керек, төменде /etc/apache2/sites-available/owncloud.conf файлына келесі жазуды қосу керек:

```
# sudo nano /etc/apache2/sites-available/owncloud.conf
Alias /owncloud "/var/www/owncloud/"
<Directory /var/www/owncloud/>
Options +FollowSymlinks
AllowOverride All
<IfModule mod_dav.c>
Dav off
</IfModule>
SetEnv HOME /var/www/owncloud
SetEnv HTTP_HOME /var/www/owncloud
</Directory>
```

Келесі Apache модульдерін қосу қажет:

```
# sudo a2enmod rewrite
# sudo a2enmod headers
# sudo a2enmod env
# sudo a2enmod dir
# sudo a2enmod mime
```

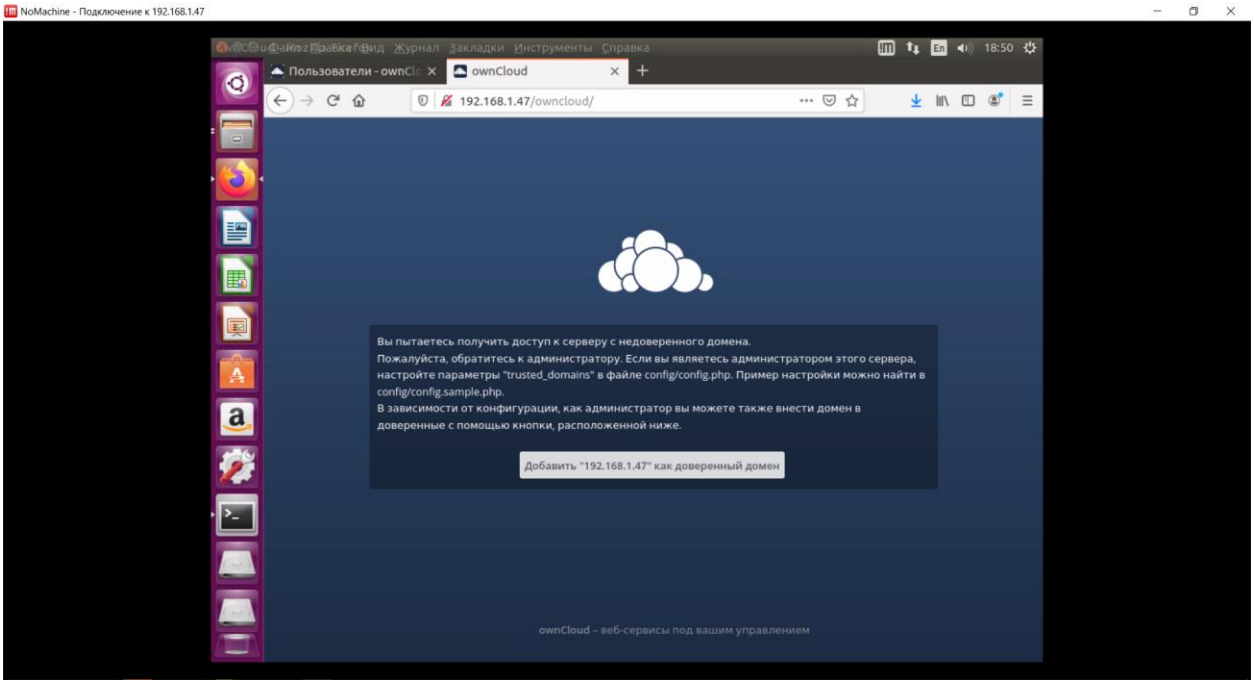
Apache OwnCloud конфигурациясын қосамыз:

```
# sudo a2ensite owncloud.conf
```

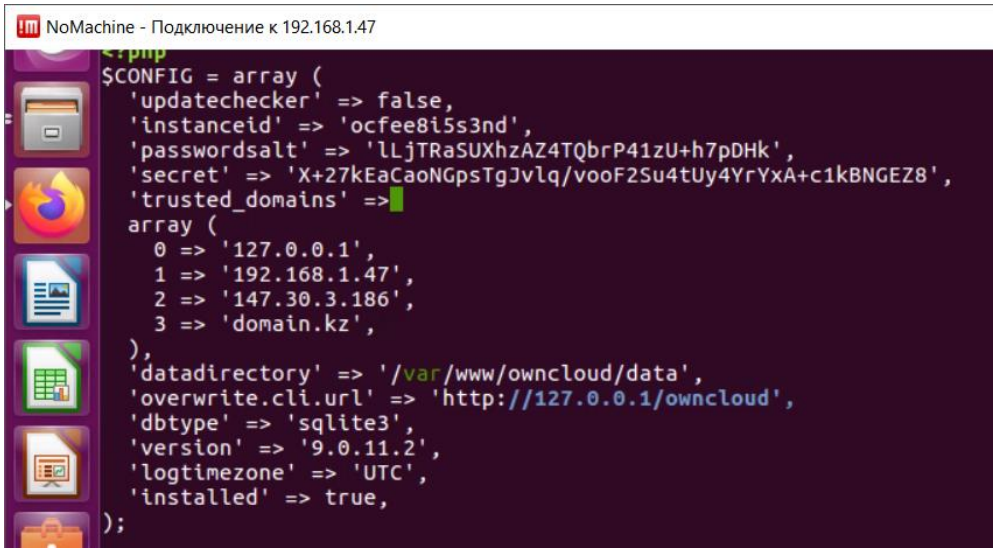
Енді Apache веб серверін қайта іске қосамыз:

```
# sudo systemctl restart apache2
```

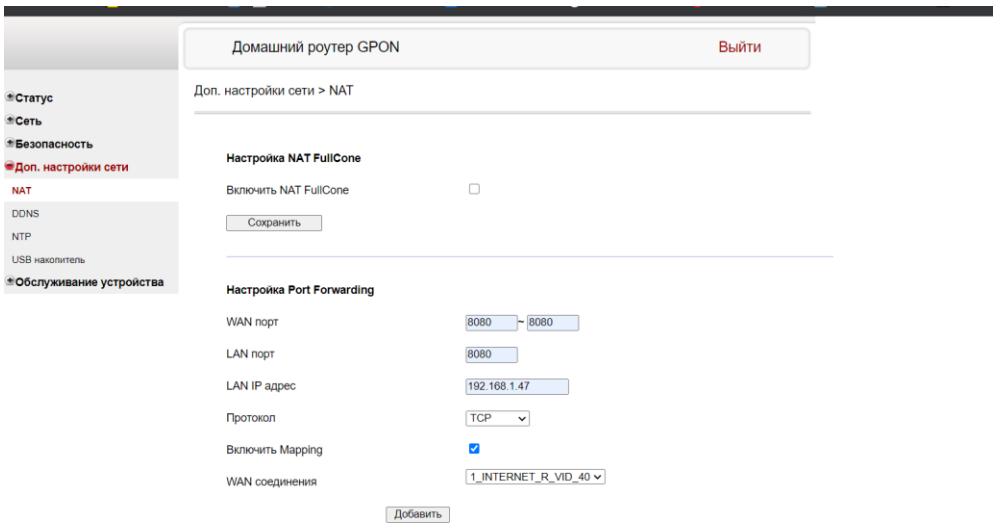
Локальды және сытрқы желіден кіру мүмкүндігін ие болу үшін біз OwnCloud және роутер баптауларына өзгертуіміз қажет. Алдымен OwnCloud баптауларына жаңа мекен жайларды енгізуден бастап, кейінен роутер баптауларын сервер мекен жайын енгізуіміз қажет.



3.21 сурет – OwnCloud-қа жаңа мекен жай қосу

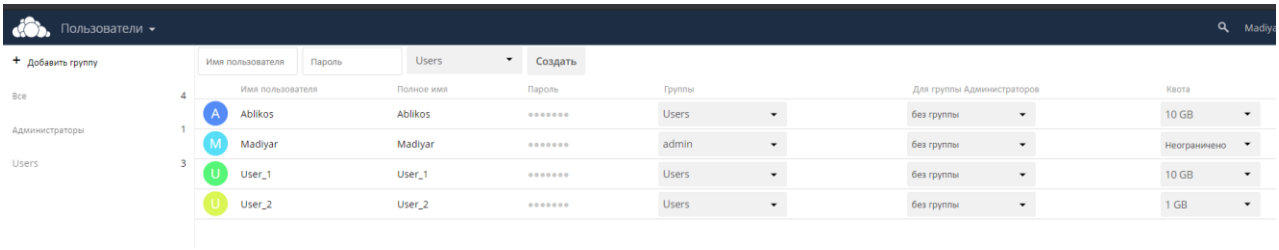


3.22 сурет – OwnCloud-қа баптауларына жаңа мекен жай қосу



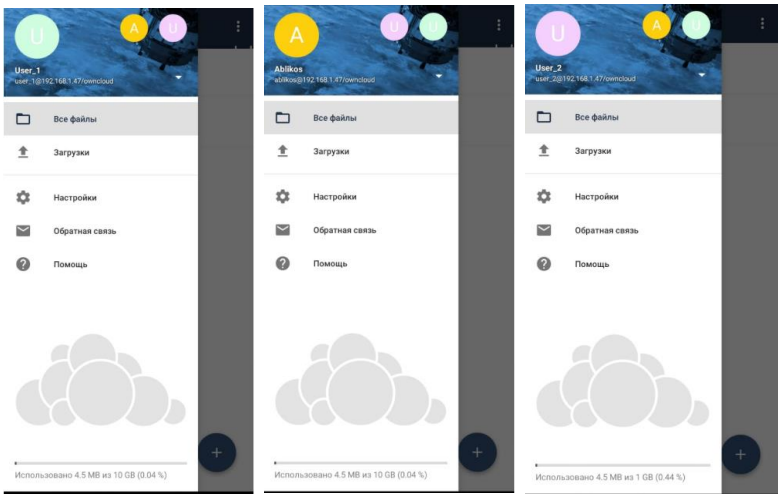
3.23 сурет – Роутерге қосымша сервер мекенжайын қосу

OwnCloud мүмкіндіктреінде әр қолданушыларға жад көлемін беруге және топтарға байланысты қолданушылар мүмкіндіктерін шектеуге болады. Енді біз үш қолданушы енгізіп оларды User тобына тіркедік, ал негізгі қолданушы admin тобына тіркелген.



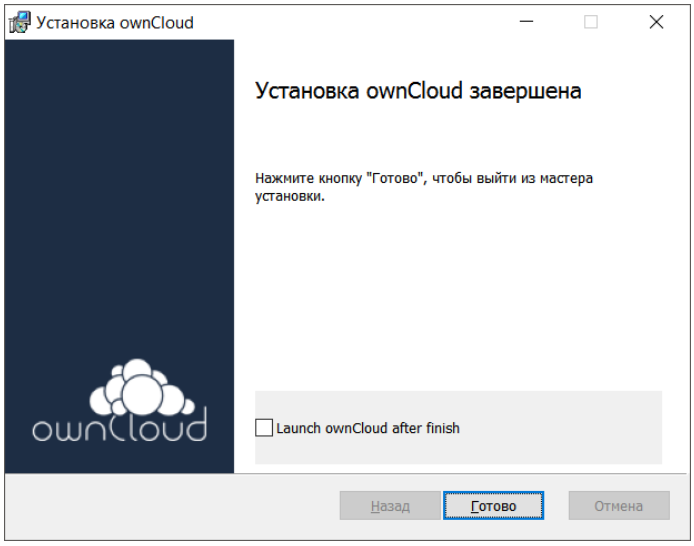
3.24 сурет – OwnCloud қолданушылары мен топтары

Өзгертулер енгізгеннен кейін смартфон қосымшасы арқылы тексереміз. User_1, Ablikos қолданушыларына 10 Гб және User_2 1Гб жад бөлінді.

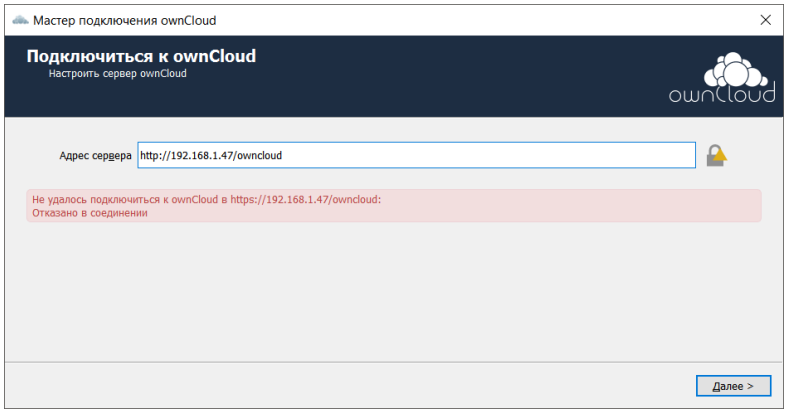


3.25 сурет – OwnCloud қолданушылары мен топтары

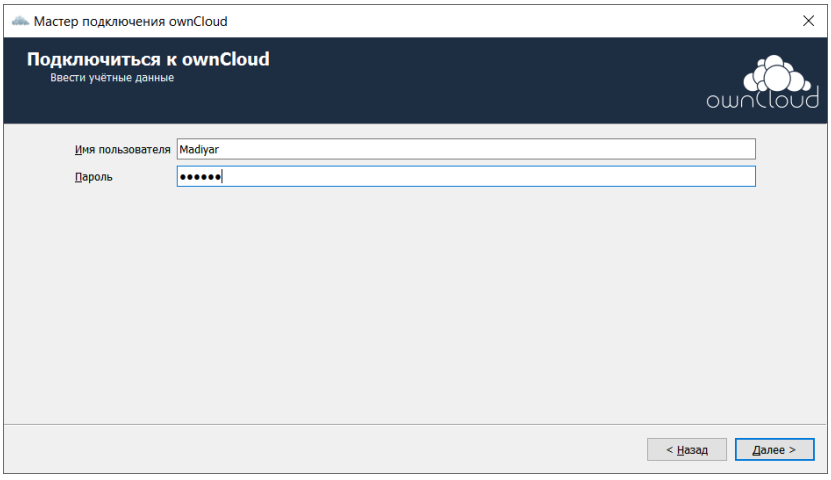
OwnCloud клиенттік бағдарламаны орнату және баптау барысы.



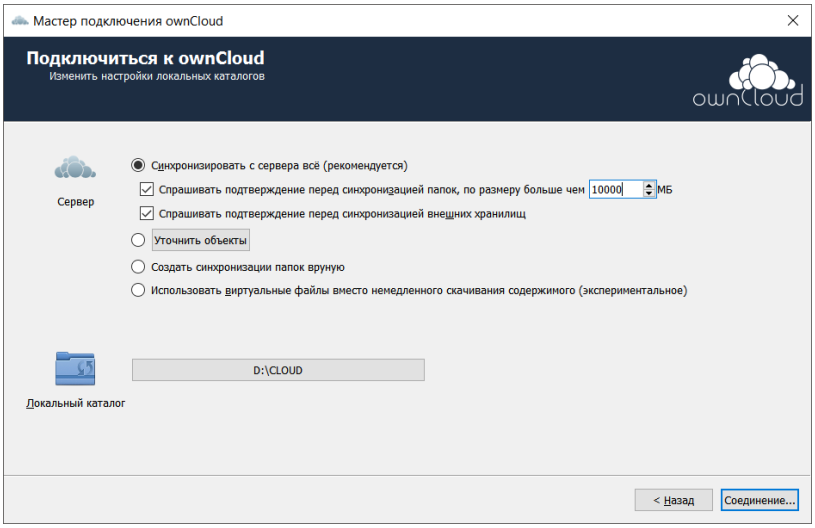
3.26 сурет – OwnCloud бағдарлама орантылуы



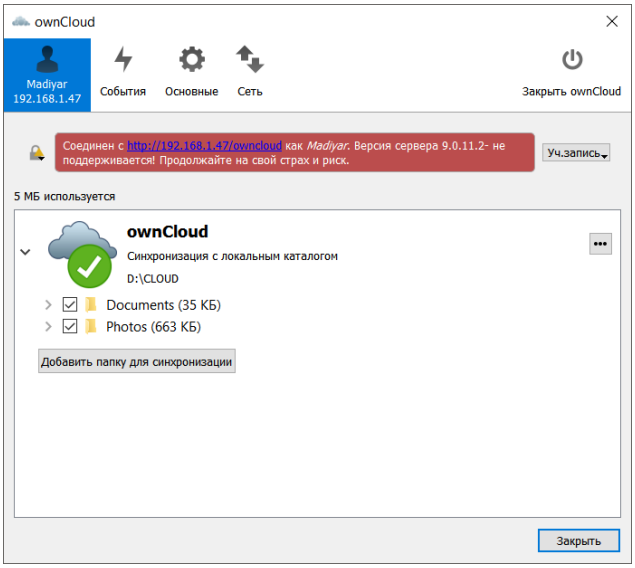
3.27 сурет – OwnCloud сервер мекен жайын енгізу



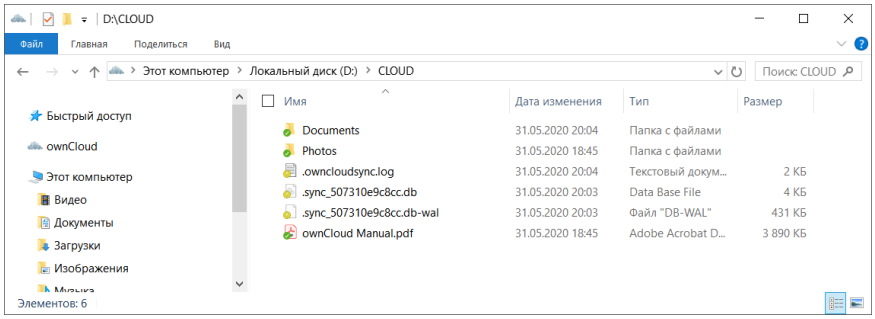
3.28 сурет – Қолданушы мәліметтерін енгізу



3.29 сурет – Локальды каталогтарды реттеу



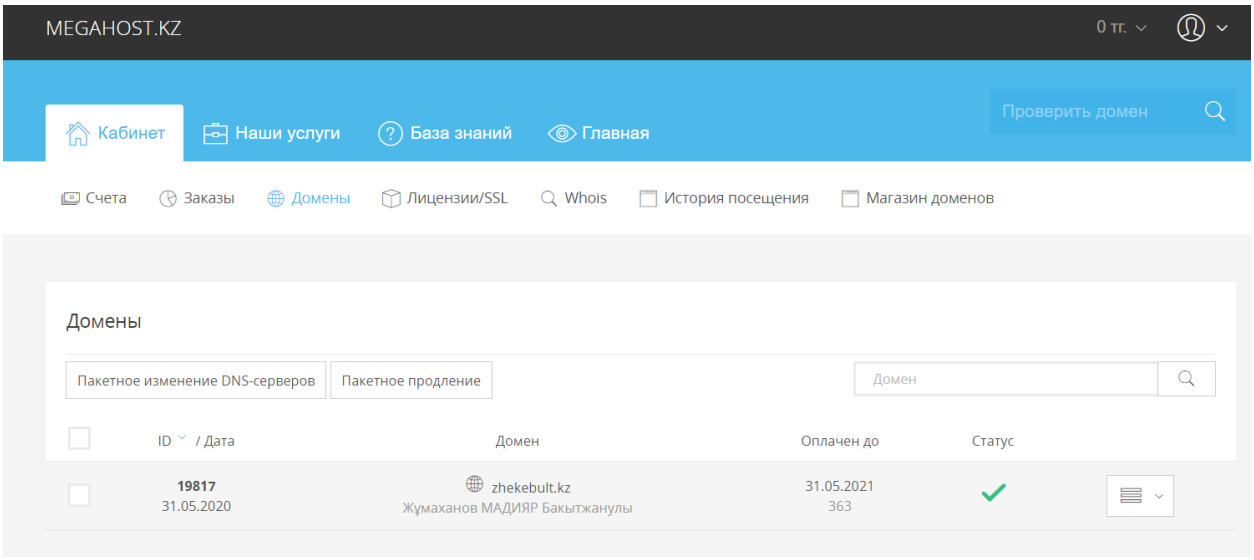
3.30 сурет – Деректер алмасу каталогын таңдау



3.31 сурет – Деректер алмасу каталогы

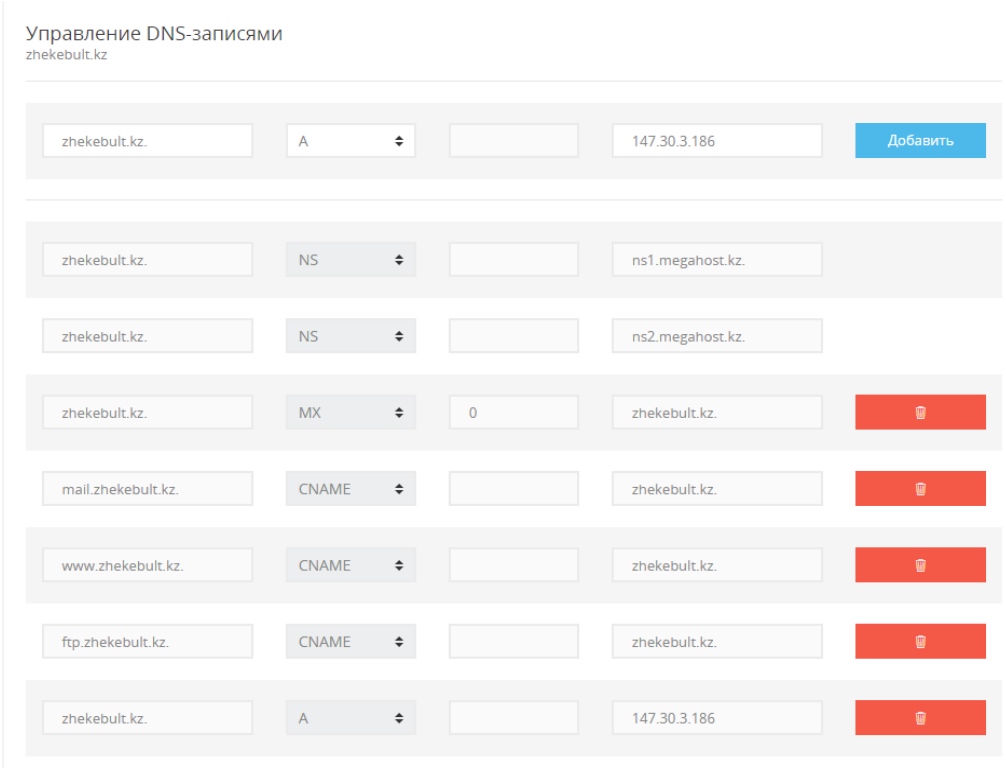
3.4 SSL сертификатын алу

Интернет желісінен жеңіл табу үшін және кейіннен SSL сертификатын алу үшін доменді сервер IP мекен жайына тіркеу керек болды. Сол себепті домен алынып роутер сытрқы IP мекен жайына тіркелінді.

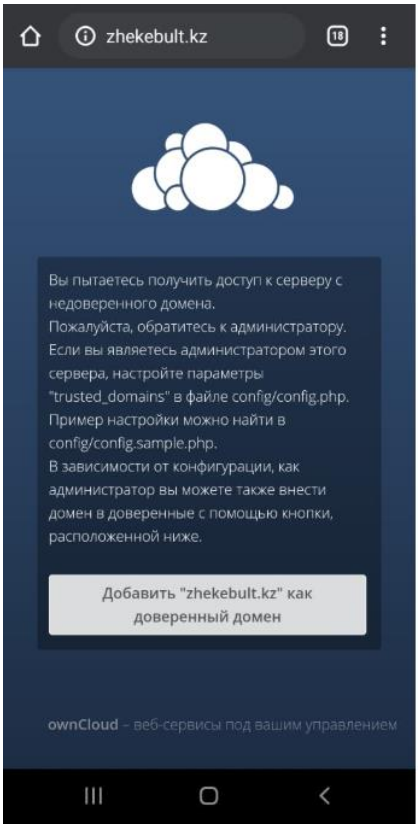


3.32 сурет – Домен баптаулары

Доменге бағыттыалған сұранымдар серверге бағытт алуы үшін, қосымша А жазба қосу қажет.

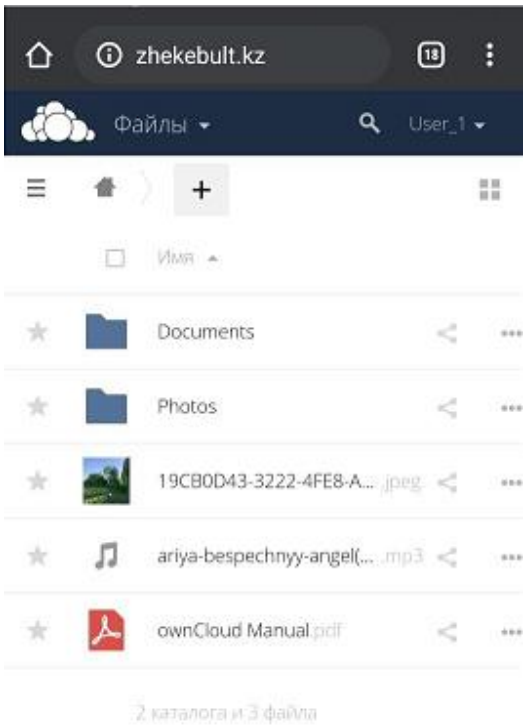


3.33 сурет – Доменге А жазба қосу



3.34 сурет – Доменді тексеру

Доменді OwnCloud баптауларына енгізгенен кейін, User_1 қолданушы атынан кірдік.



3.35 сурет – Доменді тексеру

Жасалған жұмысты қортындылай келе бұндай шешім тек кішкентай немесе енді дамушы қаражаты шектеулі компанияларға тиімді екендігін аңғаруға болады. Себебі, компания бұлтты ортаны толықтай өзі басқарады, құпия ақпарттар тек өзінің серверінде сақталады, локальді желі ішінде жұмыс деректермен жылдам алмасуға мүмкүндік береді және әр қолданушыларды топтарға бөлу арқылы құқықтарын шектеуге болады. Жәнеде, бұндай бұлт қауіпсіздігі басқа шешімдерге қарағанда жоғары болады. Ал, жұмыс күйінде ұстау үшін бөлек маманның, бөлек бөлменің қажеттілігі жоқ.

Бұл жеке бұлтты құру арқылы біз бұлтты технологияларға ауысу процессі қымбат және қиын емес екендігін дәледедік. Болашақта барлық технологиялар бұлтты оратамен байланысты болғандықтан, қазігі күнен бастап барлық компаниялар сол бағытты алу қажет.

4 Өмір-тіршілік қауіпсіздігі бөлімі

4.1 Жұмыс жағдайын талдау

Бұл дипломдық жұмыстың тақырыбы − «Бұлттық сервистер қауіпсіздігіне мониторинг жасау және зерттеу жасаймын». Жұмыс тақырыбы бойынша жұмысшыларға төрт дербес компьтер орнатылған және де байланыс желісі ретінде желілік модем қолданылады. Дербес компьютерлер желіге Wi-Fi немесе желілік сым арқылы ғаламторға шыға алады. Бұл бөлмеде жұмыс орнының желдету жүйесі мен жыбыс өткізбеу жүйесі талапқа сәйкес келеді, өйткені онда шулы құрылғылар жоқ және қазіргі уақыттағы кондиционер ауа температурасын, ауа ылғалдылығын сақтайды. Осы себепті дипломдық жұмыстың бұл бөлімінде жерге тұйықтағыштарды қажеттілікті анықтауды және алғашқы өрт сөндіру құралдарына қажеттілікті анықтауды есептеп, екі программистке жұмыс жасауға қолайлы жағдай жасалу туралы шешім қабылданды.

Бөлмеде келесі параметрлер бар:

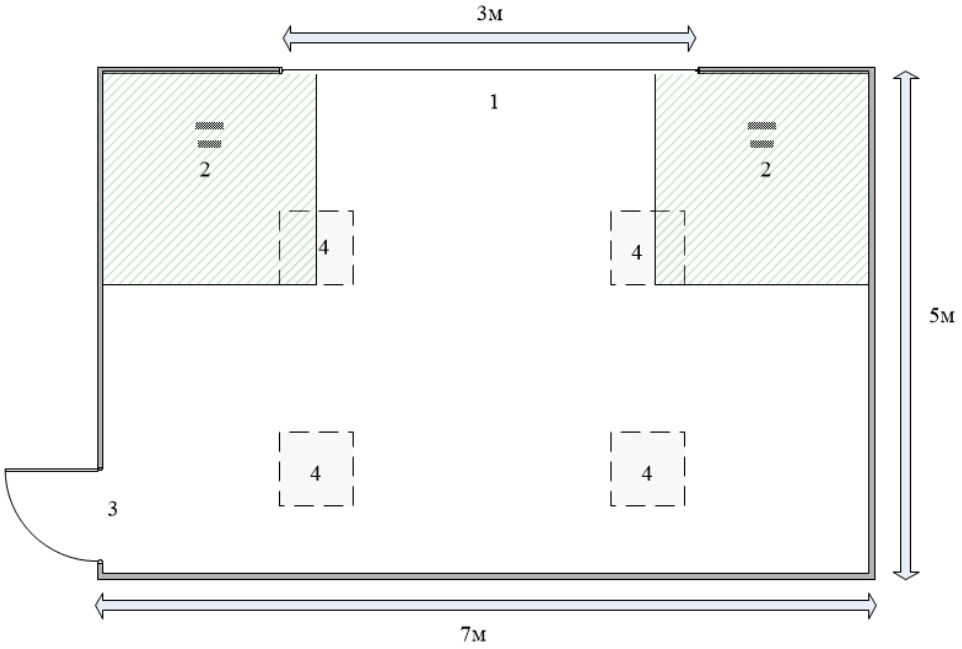
− бөлме өлшемдері: ұзындығы 7 м, ені 5 м, биіктігі 3 м;

− жарық өткізгіш материалдың түрі − шыны парағы, қос; − байланыстың түрі − болат, қосарлы, ашылады;

− терезенің өлшемі 1,8 м*0,6 м;

Көрнекі жұмыс жағдайлары бөлмесі жеңіл жұмыстардың санатына жатады (жеңіл физикалық, Іа санаты, сеанс жұмыс жасалады және физикалық күш талап етілмейді); Жасанды жарықтандыру − 4 люминесценттік шаммен.

4.1-суретте бөлменің орналасуы, онда 1 − терезе, 2 − жұмыс орны, 3 − есік, 4 – жарық шамдары.



4.1 сурет − Бөлме жоспары

4.1.1 Микроклимат

СанПиН 2.2.4.548-96 [19] қосымшасының 1-пунктіне сәйкес I санатына жатады, яғни 120 ккал / сағ энергиясынан артық емес шығын қарқындылығымен жұмыс жасайды.

Қоғамдық ғимараттарды жылыту және желдету кезінде микроклимат параметрлерін қамтамасыз ету үшін ҚР ҚНжЕ 4.02-42 [20] талаптарына және осы бөлімнің талаптарын ескере отырып жасаланады. Оңтайлы микроклимат шарттары адамның жылу және функционалдық күйіне байланысты белгіленеді және терморегулятор тетіктерінің минималды кернеулері бар жұмыс күнінің ішінде жоғары тиімділікке қолайлы жағдай туғызады. Осы санаттағы жұмыс үшін жұмыс орнындағы микроклимат көрсеткіштерінің оңтайлы мәндері 4.1-кестеде көрсетілген. Ғимараттағы суық кезеңіндегі ауа температурасы 22-23°С, ал жылы кезеңдегі температура 24°С. Беттердегі ауа температурасы суық кезеңде 23°С, жылы кезеңде 24°С-та болады. Ауаның ылғалдылығы мен ауа қозғалысының жылдамдығы 4.1 кестеде берілген микроклимат көрсеткішіне сәйкес келеді, яғни 55%-ды және 0,1 м/с құрайды. Ғимарат көрсеткіштері ҚР ҚНжЕ 4.02-42-2003 [20] талаптарына сәйкес келеді.

4.1 кесте – Оңтайлы микроклимат көрсеткіштері

Жыл кезеңі	Ауа температурасы, °С	Беттердің температурасы° С	Салыстырмалы ауаның ылғалдылығы, %	Ауа қозғалысы жылдамдығы м/с
Суық	22-24	21-25	60-40	0,1
Жылы	23-25	22-26	60-40	0,1

4.1.2 Жарықтандыру жүйесі

Жарық беретін қондырғылардың жобалауы ҚР ҚНжЕ 2.04-05-2002 [21] нұсқаудағы қабылданған жалпы қағидаларға бағынады.

Жобаның жарық техника бөлімінде жарық сапасының көрсеткішін және

жарықтандыру мағынасын, жүйесін, түрін және жарық әдістерін, жарық көздерімен жарық аспаптарын таңдауы орындалады.

Жарық аспаптарының түрі, қуаты және орналасуы жарық техникалық есептің нәтижесі бойынша таңдап алынады.

Жобалаудың тәжірибесінде жарық беретін қондырғылардың бірнеше сипаттамасының өзгешелігі (әртүрлі жарық жүйесі, әртүрлі шамдар мен жарық көздерінің типтері, шамдарды орнатудың әртүрлі биіктігі) арқылы ерекшеленеді.

Адамдардың қызмет етуіне жеткілікті табиғи және жасанды жарықтандыру атқарылатын жұмыстардың жоғары сапалылығын, қауіпсіздікті қамтамасыз етеді, еңбек жағдайларын жақсартып өнімділігін арттырады, салдарынан, жұмыс

жасаушылардың психологиялық күйіне әсер етеді. Жұмыс орнындағы жарықтың жеткіліксіздігі адам денсаулығына кері әсерін тигізеді, шаршап-шалдығу ұлғаяды, еңбек өнімділігі төмендейді, жарақат алу жиілеп, ауырлығы көбейеді. Жұмыс орындарын жарықтандыру сапасы көру жағдайы мен бағаланады да мына жағдайлармен сипатталады:

– үнемі жарықтандырылумен;

– кереғарлықтың болмауы;

– бетті және қоршаған кеңістікті жарықтандырудың жеткілікті және біркелкі таралған жарықтықтың болуы;

– көзді шағылдырмау;

– жарық түсетін беттерде айқын және терең көлеңкелердің болмауы.

Жасанды жарықтандыру үшін энергия үнемдейтін жарық көздерін пайдаланады. Тең қуаттылық кезінде, ұзақ мерзім қызмет атқаратын және ең көп жарық беретін жарық көздеріне жол беріледі. Жалпы қолданыстағы 100Вт және одан жоғары қуатты қызу лампаларын жарықтандыруға пайдалануға тыйым салынады.

4.1.3 Өрт қауіпсіздігі

Өртке қарсы су қондырғыларына қойылатын талаптар ҚР ҚНжЕ 2.02-05-2009 [22] құрылыс проект нормасымен анықталады. Электр тораптарына, соның ішінде электронды компьютерлерге қосылатын әртүрлі мақсаттағы құрылғылармен жұмыс істеу кезінде қадағаланды. Дұрыс жасалған құжат электрлік құрылғылармен жұмыс бөлмесінде сипаты дұрыс емес жағдайлардан туындайтын қауіпті жағдайларды болдырмауға көмектеседі.

Монитордан және жүйелік блоктан шығатын кабельдер, сондай-ақ CRT мониторларындағы жарық түтігі жұмыс істеп тұрған электр кернеумен жұмыс

істейді. Осы құрылғыларды абайлап, дәлме-дәл пайдалану шкафта өрттің пайда болуына немесе адамның электр тогына түсуіне себеп болады.

Осыдан жұмыс компьютерлік кабинетінде мінез-құлық ережелерін сақтаңыз:

− тек таза, құрғақ қолдармен электр құрылғылармен қолдану;

− жұмыс аймағына кірмеңіз;

− ақаулы түрі бар электр сым ашасын розеткаға салуға тыйым салынады;

− жұмыс үдерісі кезінде сымның қыздыру дәрежесін бақыланады;

− қосқыштарды, қуат сымдарын, жерге тұйықтау құрылғыларын,

− монитордың артқы жағына түртуге тыйым салынады;

− жабдықты өзіңіз жөндеуге болмайды;

− электр лампаларының бетіне қағаз, шүберек және басқа да жанғыш материалдарды қоюға тыйым салынады;

− жоғарғы қуатты электр құрылғыларын бір розеткада қосуға болмайды;

− егер құрылыс кодекстерімен көзделмесе, сыныпқа жиһаз және

− жабдықты қайта өңдеуді жүзеге асыруға тыйым салынады;

Егер ғимарат өртеле бастаған болса:

− барлық электронды жабдықты ажыратыңыз;
− өртті жою үшін сақтық шараларын қолданыңыз;
− мүмкіндігінше материалдық активтерді босату;
− қажетті қызметтерге өрт туралы есеп беру − кезекші, басқарушы
− бақылау пункті.

Мұндай жағдайда, егер электрлік кернеу ДК-ның металл бөліктерінде немесе жердегі сымдарда анықталса, жабдықты кешіктірусіз ажыратыңыз. Компьютерлік сыныпта жұмыс істейтін адамдар электр тогынан зардап шегетін адамдар мен күйіктерден зардап шеккен адамдардың басымдықты шараларын біледі.

4.1.4 Электр қауіпсіздігі

Қоғамдық ғимараттардың электротехникалық құрылғылары Қазақстан Республикасының электр қондырғыларын орнату ережесіне, ҚР ҚНжЕ 2.04-01-2001 [23] талаптарына сәйкес жобаланады.

Жергілікті электр жарақаттары электр тогының дене ұлпалары мен мүшелерін зақымауы: күюлер, электр таңбалары, терінің электр металдануы және электроофтальмия (көздің қарығуы) болып табылады.

Токтың келесі шектік мәндерін бөліп атауға болады:

− токты сезу шегі –ең аз сезілетін ток (0,5 -1,5мА);

− босатпайтын ток шегі –адам өз бетімен бұлшық еттері электродтармен қамтылған әрекеттен босана алмайтын ең аз ток мөлшері (6-10мА). Бұдан аз токтар босататын болып есептеледі;

− қаза ететін (100 мА және одан астам) ток.

Изоляцияның бүлінуінің әсерінен кернеу астында қалған металды құрылымдарды немесе электр құрылғылардың корпусын ұстау нәтижесінде алынатын электрлік жарақаттарды болдырмау және аппаратураларды қорғау үшін қорғанысты жерлендіру орналастырылады. Ол электр қондырғылардың метал бөліктерін жермен әдейі жалғау арқылы жасалынады.

Жерлендіру құрылғыларын (ЖҚ) жобалау кезінде адамның электр тоғымен жарақат алу ықтималдылығы ескеріледі. Алайда, бірде-бір салада және жалпы өмірде адамдардың толық қауіпсіздігін қамтамасыз ете алмайды.

Сондықтан, ЖҚ-ның аймағында қауіпсіздікті қамтамасыз ету мәселесін адам электр тоғымен жарақат алу қаупі жағдайының болу ықтималдылығын азайтылады.

Тиімді жерлендірген желілерде электр қауіпсіздігі қамтамасыз етілген деп жерлендіргіштегі φж потенциалы 10 кВ-тан аспайтын, ал жерлендіргіштің нәтижелі кедергісі жылдың кез-келген мерзімінде 0,5 Ом-нан аспайтын болып саналады.

4.2 Есептеу бөлімі

4.2.1 Жерге тұйықтау есебі

Есеп әдістемелік нұсқауларымен жүргізілді [25]. Жұмысты электр қондырғыларын техникалық пайдалану ережелеріне сәйкес жүргізеді. Сонымен қатар электр құралдарымен жұмыс істеу кезінде қауіпсіздік техникасы бойынша кіріспе және мерзімді нұсқамалар сақталды, еңбек тәртібін орындалды , жұмыс орнын дұрыс ұйымдастыралды. Жерге тұйықталу шиналары қол жетімді жерлерде орналасқан. Қорғау үшін жабдық пен аспаптардың ток өткізгіш бөліктеріне жанасу оқшаулауды, ток өткізгіш бөліктерінің орналасуы мен қоршауын пайдаланады. Жабдықтың металл бөліктеріне жанасу кезінде кездейсоқ кернеу астында болуы мүмкін электр тогының зақымдануынан қорғау үшін, қондырғы корпусын қорғағыш жерге қосылды. Жерге тұйықтау есебін шығару үшін бастапқы деректер қажет олар 4.1 кестеде көрсетілген.

4.2 кесте – жерге тұйықтауды есептеу үшін бастапқы деректер

Топырақтың меншікті кедергісі, Ом*м	Жерге тұйықтағыштың диаметрі, d, м	Жерге тұйықтағыштың ұзындығы, L, м	Жерге тұйықтағыштың орналасу тереңдігі, h, м	Жерге тұйықтағыштар арасындағы қашықтық,	Жолақтың ені, b, м
300	0,05	2,0	0,7	6,0	0,02

Бір жерге тұйықтағыштың кедергісі мына формула бойынша анықталады:

$$R\text{тк} = \rho * (\lg (2 * L / d) + 0{,}5 * \lg ((2 * 4 * t + L) / (4t * L))) / 2 * п * L \quad (4.1)$$

мұндағы Rтк - жерге тұйықтағыштың кедергісі;

ρ – топырақтың меншікті кедергісі;

L – жерге тұйықтағыштың ұзындығы;

t – жерге тұйықтағыштың орналасу тереңдігі;

d – жерге тұйықтағыштың диаметрі.

Rтк = 300 ∗ (lg (2 ∗ 3 / 0,05) + 0,5 ∗ lg ((4 ∗ 2,2 + 3) / (4 ∗ 2,2 * 3))) / 2 * 3,14 * 3 = 15,57 Ом

Жерге тұйықтағыштың саны мына формуламен есептеледі:

$$n = R\text{тк} / R\text{нк}, \quad (4.2)$$

мұндағы, n - жерге тұйықтағыштың саны;

Rтк - жерге тұйықтағыштың кедергісі;

Rнк - нормалар бойынша жерге тұйықтағыштың кедергісі (4 Ом).

Жерге тұйықтағыштар арасындағы қашықтық мынадай формула бойынша есептеледі:

$$a = 2 * L \qquad (4.3)$$

мұндағы, а - жерге тұйықтағыштардың арақашықтық;

L - жерге тұйықтағыштың ұзындығы.

$$a = 2 * 3 = 6 \text{ м}$$

Олардың өзара экрандалуын ескере отырып, жерге тұйықтағыштардың саны мынадай формула бойынша анықталады:

$$\text{nЭ} = n/\eta_{\text{жс}} \qquad (4.4)$$

мұндағы, $n_э$ - өзара экрандалуын ескергендегі жерге тұйықтағыштар саны; n - өзара экрандалуын ескермегендегі жерге тұйықтағыштар саны; $\eta_{\text{жс}}$ - жерлендіргіштерді өзара экрандалуын ескеретін пайдалану коэффициенті.

$$n\text{э} = 4/0{,}88 = 5$$

Жерге тұйықтау өткізгіштерінің ұзындығы мынадай формула бойынша анықталады:

$$Ln = 1{,}05 * a * n_э \qquad (4.5)$$

мұндағы, Ln - жерге тұйықтағыш өткізгіштердің ұзындығы; а - жерге тұйықтағыштардың арақашықтық; $n_э$ - өзара экрандалуын ескергендегі жерге тұйықтағыштар саны;

$$Ln = 1{,}05 * 6 * 5 = 31{,}5 \text{ м}$$

Жерге тұйықтағыш өткізгішінің кедергісі мынадай формула бойынша болады:

$$R\text{п} = \rho * (lg (2 * Ln / b * t)) / 2 * \text{п} * L \qquad (4.6)$$

мұндағы, Rж - жолақтық болаттан жасалған жерге тұйықтау өткізгішінің кедергісі; Ln - жерге тұйықтағыш өткізгіштердің ұзындығы; b - жерге тұйықтағыш өткізгіш жолағының ені; t - жерге тұйықтағыштың орналасу тереңдігі.

$$R\text{ж} = 300 * (lg (2 * 31{,}5 / 0{,}02 * 0{,}7)) / 2{,}5 * 3{,}14 * 2 = 30{,}03 \text{ Ом}$$

Барлық токтың ағуына кедергі жерге тұйықтау құрылғысының мынадай формула бойынша есептеледі:

$$R\text{жт} = R\text{тк}* R\text{ж} / (R\text{тк} * \eta * n + R\text{ж} * \eta_{\text{жс}} * n) \qquad (5.13)$$

мұндағы Rжт - барлық жерге тұйықтағыштың токқа ағу кедергісі.

$$R\text{жт} = 30{,}03 * 15{,}57/(5 * 30{,}03 * 0{,}8 + 15{,}57 * 1{,}1) = 3{,}41 \text{ Ом}$$

Жерге тұықтағыштардың нақты саны мынадай формула бойынша анықталады:

$$n = R\text{ж} / \eta\text{жс} * R\text{жт} \qquad (4.7)$$

ықтағыштардың нақты саны.

$$n = 15{,}57 / (0{,}88 * 3{,}41) = 5$$

Осылайша бөлмеде жерге тұйықтағыштардың нақты саны 5.

4.2.2 Жасанды жарықтандыру есебі

Жарық беретін қондырғылардың жобалауы ҚР СНиП 2.04.-05.2002 [26] нұсқаудағы қабылданған жалпы қағидаларға бағынады.

Жасанды жарықтандыру есебін жүргізу негізінен жарықтандырудың қалыпты мәнін қамтамасыз ету үшін шамдардың санын және қуатын анықтау болып табылады.

Жасанды жарықтандыру есебін төмендегі үш әдіспен жүргізуге болады: жарық ағынының пайдалану коэффициенті бойынша, нүктелік және меншікті қуат әдістері бойынша.

Есептеу барысында жалпы жарықтың біркелкі түсуін анықтауда негізінен қабырға, төбе және еденнің шағылысуын ескере отыра жарық ағынының пайдалану коэффициенті әдісі қолданылады.

Есептеу шамдардың түрлерін таңдаудан басталады. Ол жұмыс бөлмесінің өртке, жарылысқа қауіптілігі класына және ортаның жағдайына байланысты қабылданады.

Бөлмеде орнатылған шамдардың сәулеленуіндегі барлық жарық ағынына есептік бетке түсетін жарық ағынының қатынасы жарық қондырғыларындағы жарық ағынының пайдалану коэффициенті деп аталады.

$$n = \frac{F_n + F_{\text{отр}}}{n * F_\text{л}} = \frac{F_y}{n * F_\text{л}}, \qquad (4.8)$$

мұндағы Fп − шамдардан тікелей жарықтану бетіне түсетін жарық ағыны, лм;

Fотр – сол жарықтану бетіне түсетін шағылысу жарық ағыны, лм;

Fл − әрбір лампаның жарық ағыны, лм;

n – жарықтану бөлмесіндегі шамдардың саны.

Пайдалану коэффициентінің мәні бірден кіші болады, өйткені ПФЛ мәні әрқашан да мәнінен үлкен болады. Оның себебі жарық ағынының кейбір бөліктері қабырғаға, төбеге және жарық арматурасына сіңеді.

Жарық көзінің есептік ағыны төмендегі теңдеу арқылы есептеледі:

$$F = \frac{Eh * S * K * z}{N} \qquad (4.9)$$

мұндағы N – жарық көзінің саны; К – запас коэффициенті; z – минималды жарықтану коэффициенті (орташа және минималды жарықтанулардың қатынасы).

4.3 кесте – Бөлме индексі мен төбенің және қабырғалардың көріну коэффициенттеріне байланысты жарық ағынының пайдалану коэффициенті

Шам	ПВЛм		
ρп, %	30	50	70
ρп, %	10	30	50
I	η*100		
0,5	14	16	19
0,7	21	23	25
0,8	23	25	27
0,9	25	27	29
1,0	29	30	32
1,1	27	29	31
1,25	29	30	32
1,5	30	31	34
1,75	31	33	35
2,0	33	34	36
2,25	34	35	36
3,0	36	37	40
3,5	37	38	40
4,0	38	39	41
5,0	39	40	42

Есептеулерде z коэффициенті төмендегідей қабылданады: төбелері тік бұрышты орналасқан шамдар үшін − 1,15; қатар орналасқан ЛЛ шамдары үшін − 1,1; қыздыру шамдары үшін − 1,2.

Бөлменің индексі төмендегідей табылады

$$i = \frac{S}{h*(A+B)}, \qquad (4.10)$$

мұндағы A, B, S – бөлменің ұзындығы, ені және ауданы.

Төбелер мен қабырғалардың рефлексиялық коэффициенттерін 4.2-кестесінен аламыз.

Кесте 4.2-ге сәйкес, ρn = 70% және ρc = 50%. Формула (5.3) бойынша бөлменің индексін есептеп, i = 0.5 болатынын анықтадық.

Енді 4.2-кестесінен η коэффициентінің мәнін есептей аламыз. Осылайша, η =0,19.

4.4 кесте – Флуоресцентті лампалардың жарық ағынының мәндері

Шамның түрі	Жарқын ағын, лм
ЛДЦ 20	820
ЛД 20	920
ЛБ 20	1180
ЛДЦ 30	1450
ЛД 30	1640
ЛБ 30	2100
ЛДЦ40	2100
ЛД 40	2340
ЛБ 40	3000
ЛДЦ 80	3560

Бөлмелерде люминесцентті шамдар пайдаланғандықтан, коэффициент z = 1.1, коэффициент k = 1.3.

Формуланы (4.11) пайдаланып жарық ағынын анықтаймыз:

$$F = \frac{400*1,25*1,5*12}{0,21} = 42\ 857 \text{ лк}, \qquad (4.11)$$

Алынған жарық ағынының мәндерінен 4.3-кестеге сәйкес, керекті шамды таңдаймыз.

Мен ЛБ-40 шамдарын 3000 лм. асығысымен пайдаланамын. Сонда бөлмедегі шамдардың жалпы саны формула бойынша есептеледі:

$$N = \frac{42\ 857}{3000} = 14, \qquad (4.12)$$

Осылайша бөлмеде ЛБ-40 шамдар саны 14 дана.

Жұмыс орнындағы жерге тұйықтау және жарықтандыруды есептеулері жүргізілді. Есептеу кезінде жерге тұйықтау саны анықталды яғни, ол 5-ке тең болды. Ал, жарықтандыру есептуін жүгізу барысында бөлмеге қанша жарық шамдар қажеттігін анықтадық яғни, ЛБ-40 шам түрінің 14 дана керектігін анықталды. Есептеу барысында қойылған мақсат міндеттер толық орынадалып жұмыс барысына ыңғайлы жағдай отрасы белгіленді.

5 Ақпараттық қауіпсіздік тәуекелдері

5.1 Ақпараттық қауіпсіздік тәуекелдерін талдау

Дипломдық жұмыстың осы бөлігінде біз шағын бизнесте жеке бұлтты көтергеннен кейін туындайтын тәуекелдерді бағалаймыз.

ISO 27005-ақпараттық тәуекел ұғымын нақтылайды, оны активтерге, қауіптерге, осалдықтар мен залалға бөліп топтастырады. ISO 27005 сәйкес: ақпараттық қауіпсіздік тәуекелі-бұл актив немесе активтер тобының осалдығын ұйымға зиян келтіру үшін нақты қауіп төндірудің әлеуетті мүмкіндігі. Іс жүзінде әрбір тәуекел қандай да бір түрдегі залал әкеледі. Залал мәнін анықтау үшін тәуекел қатері ұғымы енгізілді. Тәуекелдерді есептеу үшін екі параметр бойынша тәуекелді бағалау әдістемесі қолданылды.

Жеке бұлт құрамына сервер, жұмыс станциялары және бұлтпен жұмыс істеу үшін бағдарламалық қамтамасыз ету кіреді. Сондай-ақ, бұған бейнебақылау және жұмыс уақытын есепке алу жүйелері кіреді. Оларды тексеру қажет, бірақ жиі бұл жеке іс-шаралар аясында орын алады.

5.1.1 Активтер

Ақпараттық қауіпсіздік тәуекелдерін талдау үдерісі активтерді анықтаудан басталады. Өйткені ол адам немесе ұйым үшін құндылығы бар және сондықтан жақсы қорғауды талап етеді. Ұйым үшін құндылықтан басқа, активтер заңды міндеттемелерді орындауға ықпал етуі мүмкін.

Ақпараттық қауіпсіздік жүйесінде активтер:

− аппараттық, бағдарламалық және коммуникациялық компоненттер;

− коммуникативтік олардың арасындағы байланыс;

− ол жүйенің функциясын бақылайтын деректер жасайды және / немесе тұтынады немесе оған түседі;

− жүйе ашылған физикалық және ұйымдық инфрақұрылым;

− жүйемен өзара әрекеттесетін және оның жұмысына әсер етуі мүмкін адам агенттері (мысалы, пайдаланушылар, жүйелік әкімшілер және т.б.).

Активтер 5.1-кестеде көрсетілген, ал олардың құрамы былайша көрінеді:

− Сервер – ақпаратты өңдеуге жауап береді

− Жұмыс станциялары – жұмыс және ақпарат алмасу үшін

− Windows 10 Pro операциялық жүйесі – жұмыс станциялары үшін

− OwnCloud – деректер алмасу үшін БҚ

− Брандмауэр – желі трафигін сүзуге арналған БҚ

5.1 кесте – Активтер тізімі

актив №	Активтің атауы	Саны	актива код
1	Сервер	1	ser
2	Жұмыс станциялары	12	pc
3	Windows 10 Pro операциялық жүйесі	12	os
4	OwnCloud	1	own
5	Желіаралық экран	1	fwa

5.2 Есептік бөлім

5.2.1 Екі параметр бойынша тәуекелдерді бағалау

Дипломдық жоба үшін екі праматетр бойынша тәуекелдерді бағалау әдісі таңдалды. Екі параметр бойынша тәуекелді бағалау әдісі өзіне кіреді:

- қауіптің болу ықтималдығын бағалау;
- ықтимал залалды бағалау.

Осы әдістеме бойынша тәуекел пайда болу ықтималдығын залалды бағалауға көбейту кезінде анықталады.

Бұл әдіс бірнеше кезеңнен тұрады. Яғни, бастау үшін біз тәуекелдердің бастапқы есебін жасауымыз керек, әрі қарай қолайсыз тәуекелдерге арналған шараларды анықтау керек, кейін қайтадан есеп айырысамыз. Тәуекелдердің бастапқы есебі қауіптің туындау ықтималдығын және ықтимал залалды анықтау үшін қажет. Ол үшін біз 5.2 кестені қолдануымыз керек, онда есептеу үшін қауіптің туындау ықтималдығының мәні және оның уақыт арақатынасы сипатталған.

5.2 кесте – Қауіптің туындау ықтималдығының мәні

Қауіптердің туындау ықтималдығы шкаласы	
Ықтималдылық деңгейі	Қауіптің туындау ықтималдығы
0 – өте төмен	Бірнеше жылда бір рет
1 – төмен	Жылына бір рет
2 – орташа	Бірнеше айда бір рет
3 – жоғары	Айына бір рет
4 – өте жоғары	Айына бірнеше рет

Залалды анықтау үшін 5.3-кестені пайдалану қажет, онда есептеу үшін залалдың мәні және оның ақшалай баламадағы арақатынасы сипатталған.

5.3 кесте – Залалдың мәні және оның ақшалай баламадағы арақатынасы

Шығын көлемінің шкаласы	
Мәні	Сипаттамасы
0 – өте төмен	15 000 тг дейін
1 – төмен	25 000 тг дейін
2 – орташа	50 000 тг дейін
3 – жоғары	75 000 тг дейін
4 – өте жоғары	100 000 тг жоғары

Тәуекелдерді бағалау нәтижелері (5.4 кесте):

№	Қауіптер	Осалдықтар	Тәуекелдің ең жоғары деңгейі	Тәуекелді өңдеу жөніндегі шаралар	Тәуекелдің қалдық деңгейі
1. Сервер					
1.1	Электрмен қоректендіруді ажырату, жүйе жұмысының істен шығуы	Сервер резервтік генераторға қосылмаған	6	Резервті қуат көзі	0
1.2	Рұқсатсыз кіру үшін зиянды БҚ жұқтыру	Қызметкерлердің біліктілігі жеткіліксіз	6	StoneGate IPS 1060-жүйесі , сақтық көшірме	1
1.3	Уақытында қызмет көрсетілмегендіктен деректерді жоғалту, істен шығару	Сервердің техникалық жай-күйіне тұрақты емес қызмет көрсету	5	Жұмыстарды жоспарлаушы	0
2. Рабочие станции					
2.1	Қатты диск (деректер) алу үшін қасақана істен шығару)	Недостаточное физическая защита и контроль за сотрудниками	3	Veracrypt	1
2.2	БҚ жұмысының істен шығуы	БҚ жәнежабдықтарды нашар оңтайландыру	2	Қажет емес	2
2.3	Тыңшылық бағдарламалар	Құпия ақпаратты ұстап қалу	6	Dr.Web – антивирусты БҚ	1
3. ОС Windows 10 x64 Pro					

3.1	ОЖ қашықтан басқару	Жаңартылмаған ОЖ(EternalBlue осалдығы)	5	Dr.Web – антивирусты БҚ	2
3.2	ОЖ жұмысының істен шығуы	ОЖ нашар оңтайландыру, жаңартуы сонгы нұсқа емес	5	Dr.Web – антивирусты БҚ	2
3.3	ОЖ жұмыс үрдістері мен режимдерінің өзгеруі	БҚ дұрыс пайдаланбау	6	Dr.Web – антивирусты БҚ	2
4. OwnCloud					
4.1	Жеке деректерді ұрлау	Бағдарламалық кодында осалдылық	3	Dr.Web - антивирусное ПО	2
4.2	Буфердің толып кету шабуылдары	Алмасу буфері үшін таңдалған жады дұрыс емес	3	Dr.Web - антивирусное ПО	1
4.3	Қаржылық пайда алу үшін бағдарламалық кодты қасақана өзгерту	Қызметкерлерді қаржылық көтермелеудің жеткіліксіздігі	6	Dr.Web - антивирусное ПО	2
5. Желіаралық экран					
5.1	Буфердің толып кету шабуылдары	Трафик ағынын дұрыс емес баптау	3	StoneGate IPS 1060-система	1
5.2	Деректерді жинау үшін желілік трафикті ұстап қалу	Желілік инфрақұрылымды	2	не нужно	2

		құрудағы осалдықтар			
5.3	Қызметкерлердің қасақана іс-әрекетіне байланысты істен шығару, қате жұмыс	Желіаралық экран интерфейсіне кіру үшін стандартты параметрлер	6	StoneGate IPS 1060-система	1

Осы кестеде біз қорғау шараларын қолданғанға дейін және кейін тәуекелдердің есебін жүргіздік. Қауіпсіздікті қамтамасыз ету үшін әр түрлі қорғау жүйелерін енгізу жүргізілді, олар кейіннен тәуекелдерді төмендетуге көмектесті. Нәтижесінде біз осы есептеу әдісі тәуекелдердің ауқымын бағалауға жақсы көмектесетініне көз жеткіздік және осының негізінде қауіпсіздікті қамтамасыз ету бойынша шаралар қабылданды.

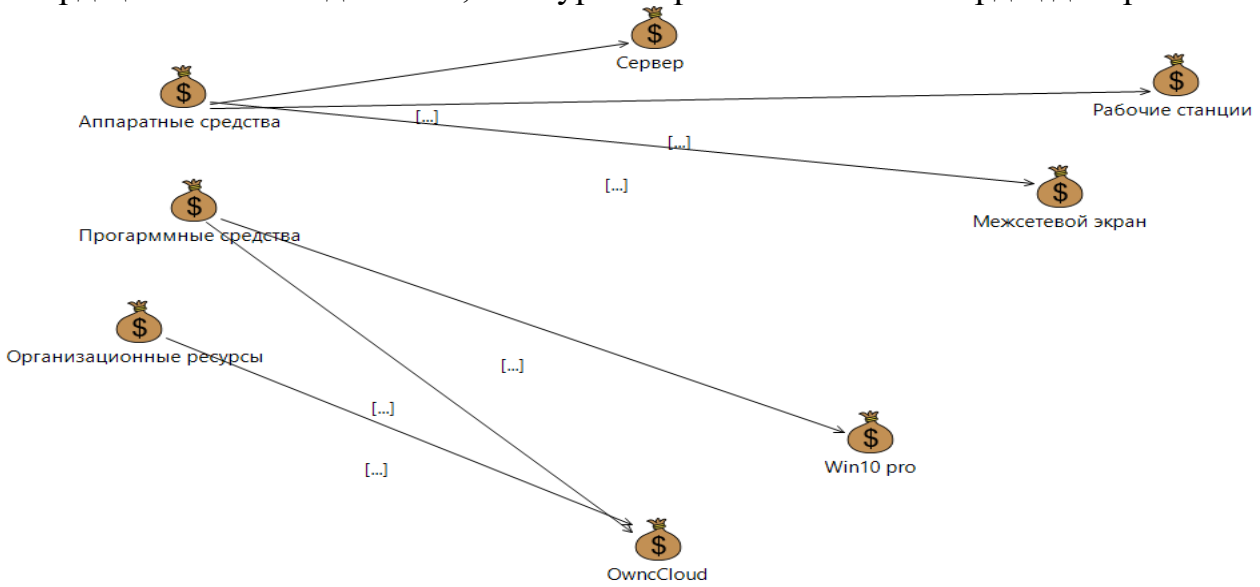
5.2.2 CORAS әдістемелерінің ақпараттық қауіпсіздік тәуекелдерін талдау

CORAS [1] методологиясы Information Society Technologies бағдарламасы аясында әзірленген. Оның мәні Event-Tree-Analysis, Марков тізбегі, HazOp және FMECA [2] сияқты тәуекелдерге талдау жүргізу әдістерін бейімдеу, нақтылау және біріктіруден тұрады.

CORAS UML as / as as / NZS 4360 технологиясын қолданады: 1999 code ISO/IEC 17799-1: 2000 ақпараттық қауіпсіздікті басқару тәжірибесінің кодексі. Guidelines, Guidelines ISO / IEC TR 13335-1: 2001 ат қауіпсіздігін басқару және IEC 61508: 2000 қауіпсіздікке байланысты электр / электрондық/бағдарламаланатын қауіпсіздіктің функционалдық қауіпсіздігі.

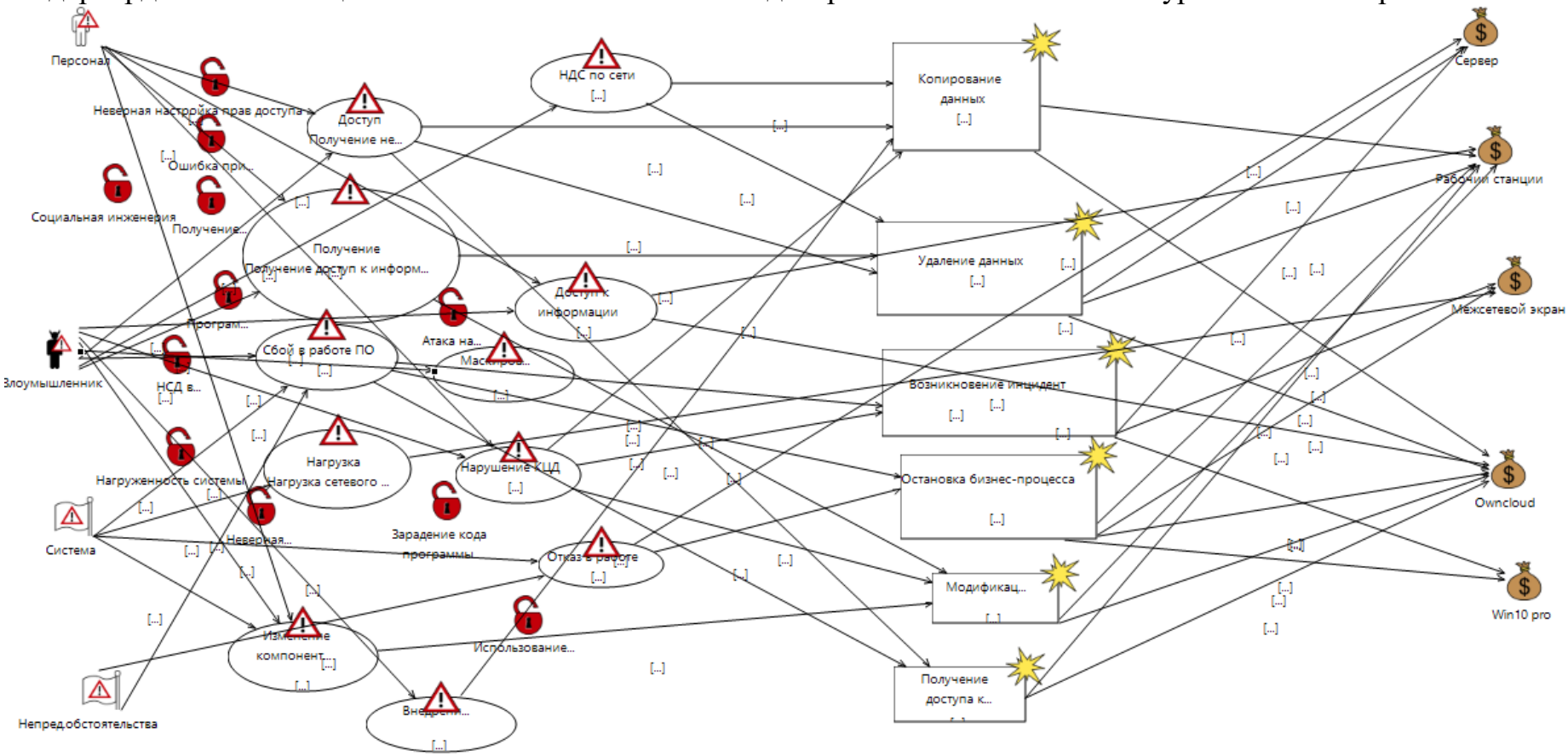
CORAS-қа сәйкес Ақпараттық жүйелер пайдаланылатын технологиялар тұрғысынан ғана емес, бірнеше жағынан, атап айтқанда адам факторы ескерілген күрделі кешен ретінде қарастырылады. Бұл әдістеменің ережелері Windows және Java-қосымшалар түрінде іске асырылған.

Активтердің тізбесін пайдаланып, 5.1-суретте ұсынылған активтердің диаграммасын құрдық.



5.1 сурет – Активтер

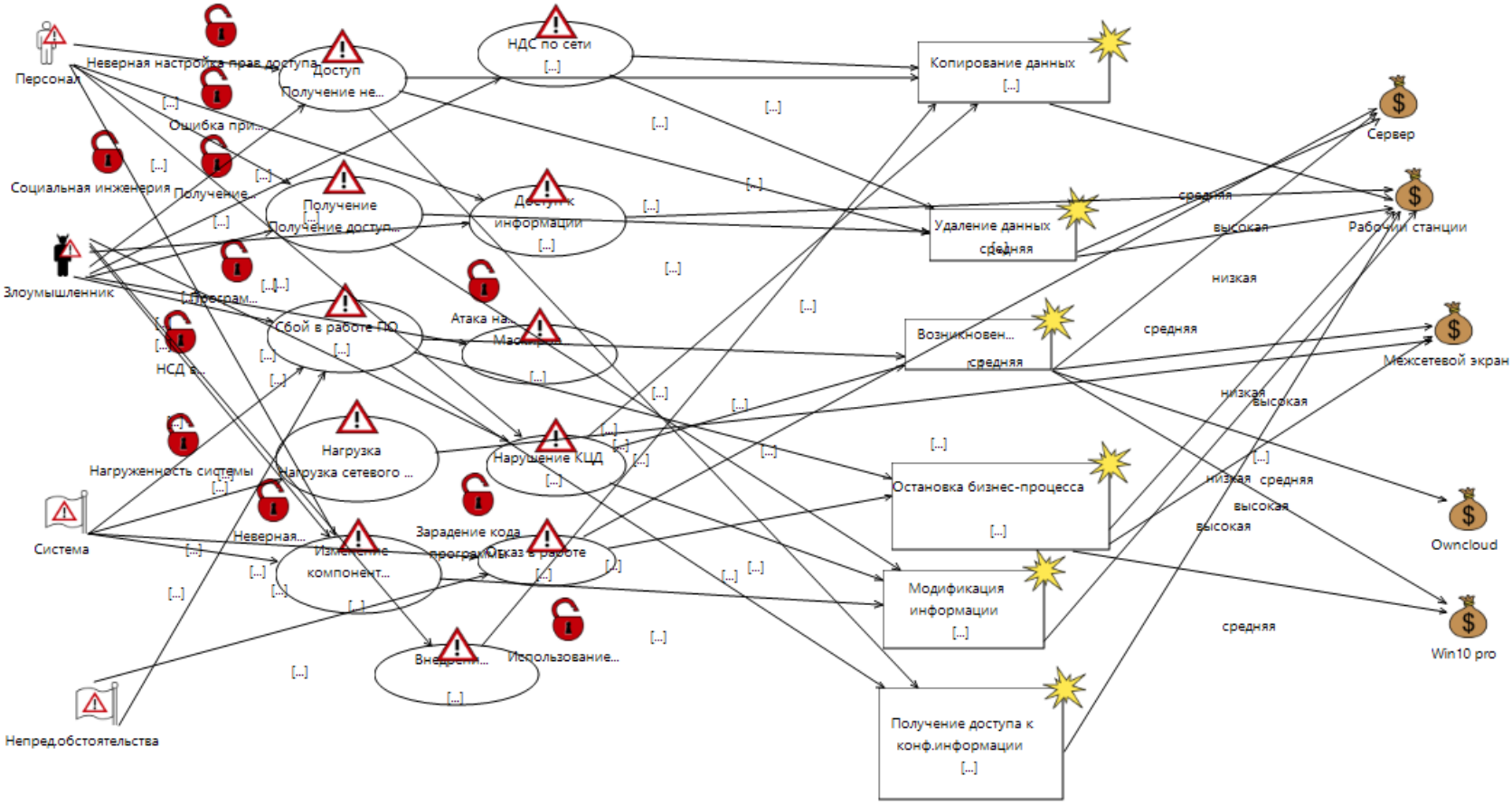
5.4 кестені пайдалана отырып, қауіптер моделін құрдық. Тәуекелдер диаграммасын генерациялаймыз,бұдан әрі әрбір актив үшін әрбір тәуекел бойынша осы тәуекел жүзеге асырылған жағдайда салдарларды анықтаймыз. Алынған диаграмма 5.2 суретте көрсетілген.



5.2 сурет – Қауіптер моделі

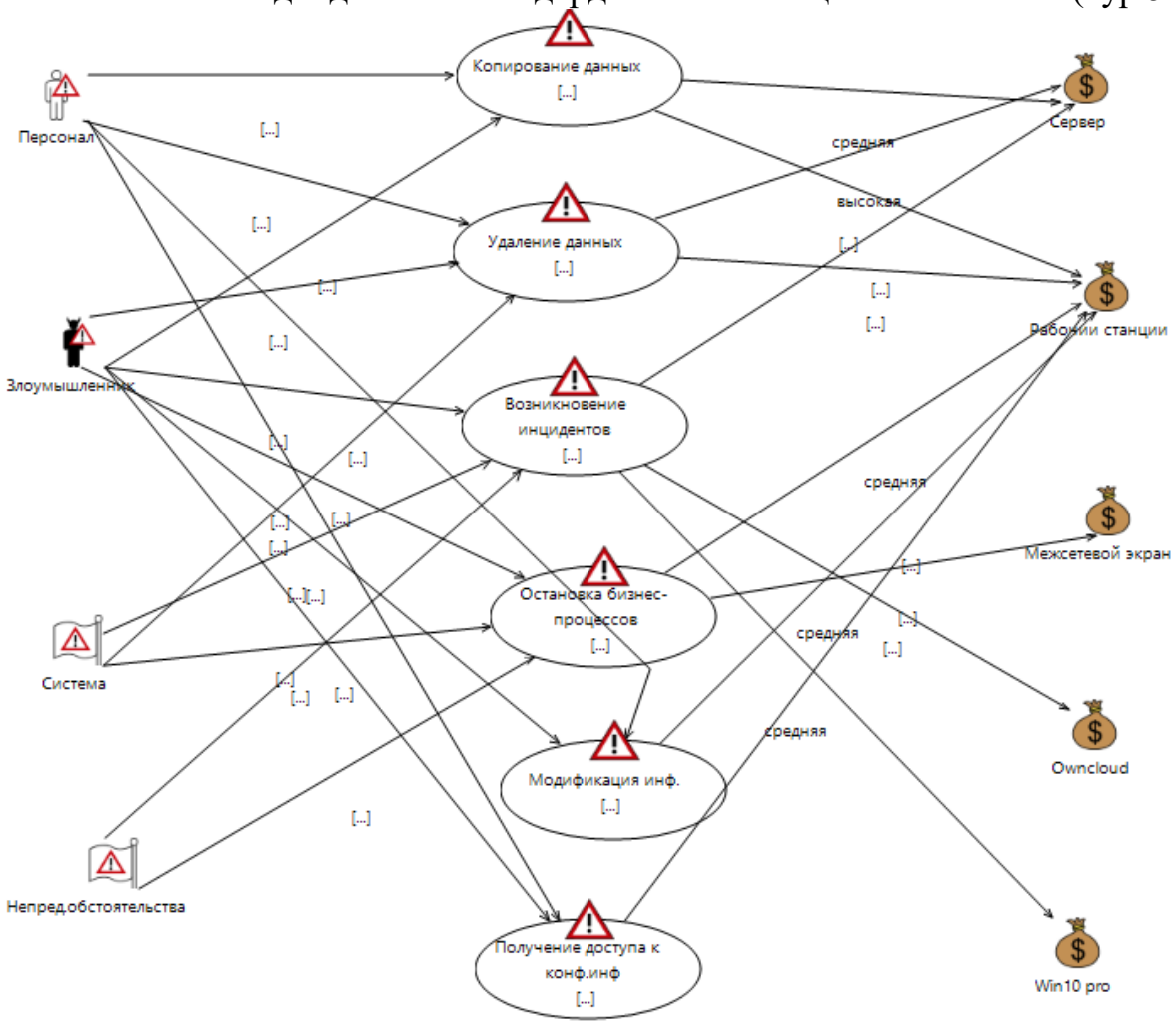
Алдыңғы қадамда алынған модельге жағымсыз инциденттің сценарийін жүзеге асыру ықтималдығын келтіреміз.

Нәтижесінде қатерлердің толық моделін аламыз. Біздің мысал үшін бұл қауіп моделі күріш ұсынылған.5.3.



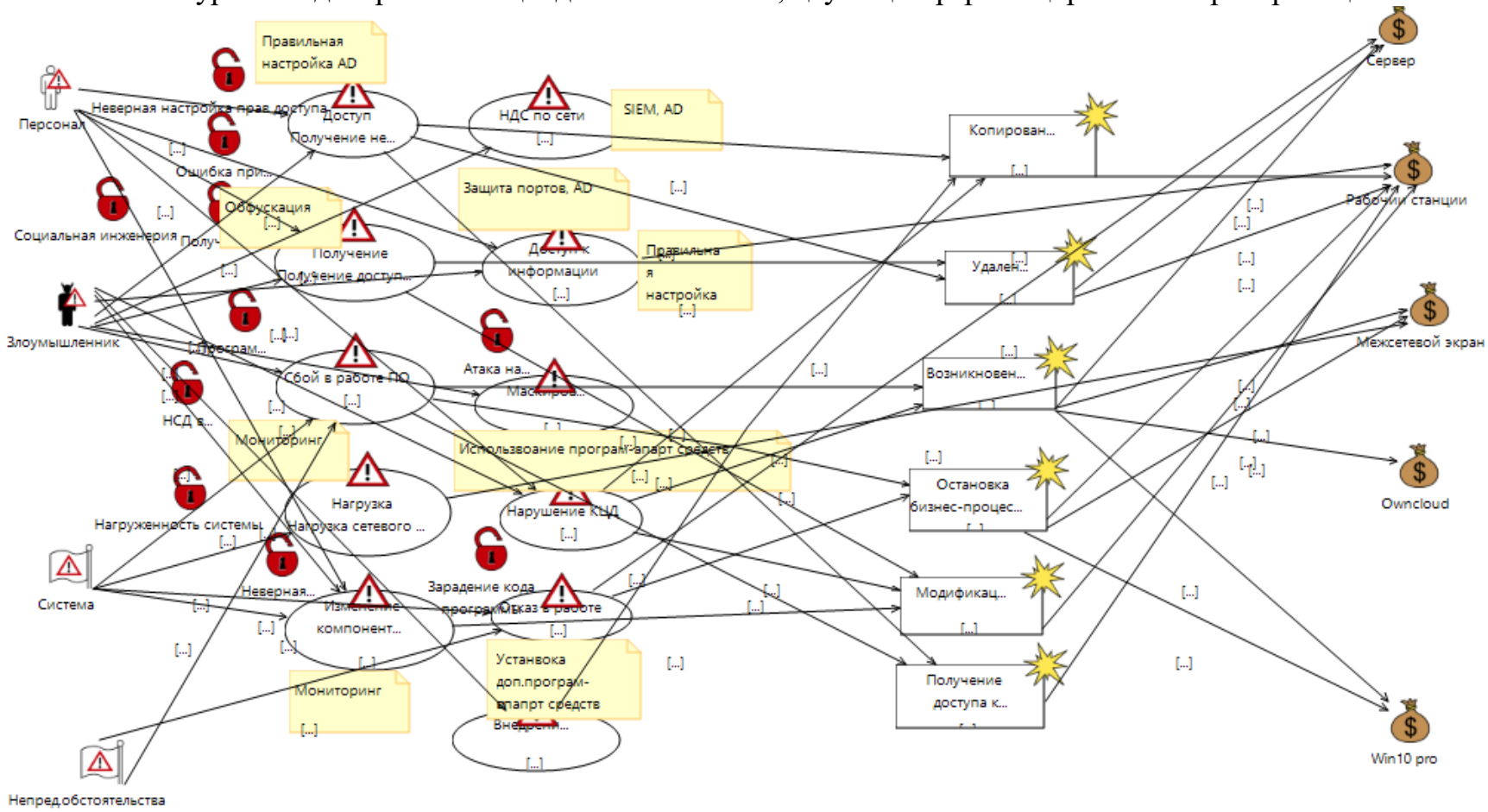
5.3 сурет – Тәуекелдер диаграммасы

Енді әрбір тәуекел бойынша әрбір актив үшін осы тәуекел жүзеге асырылған жағдайда салдарды анықтаймыз. (сур.5.4).



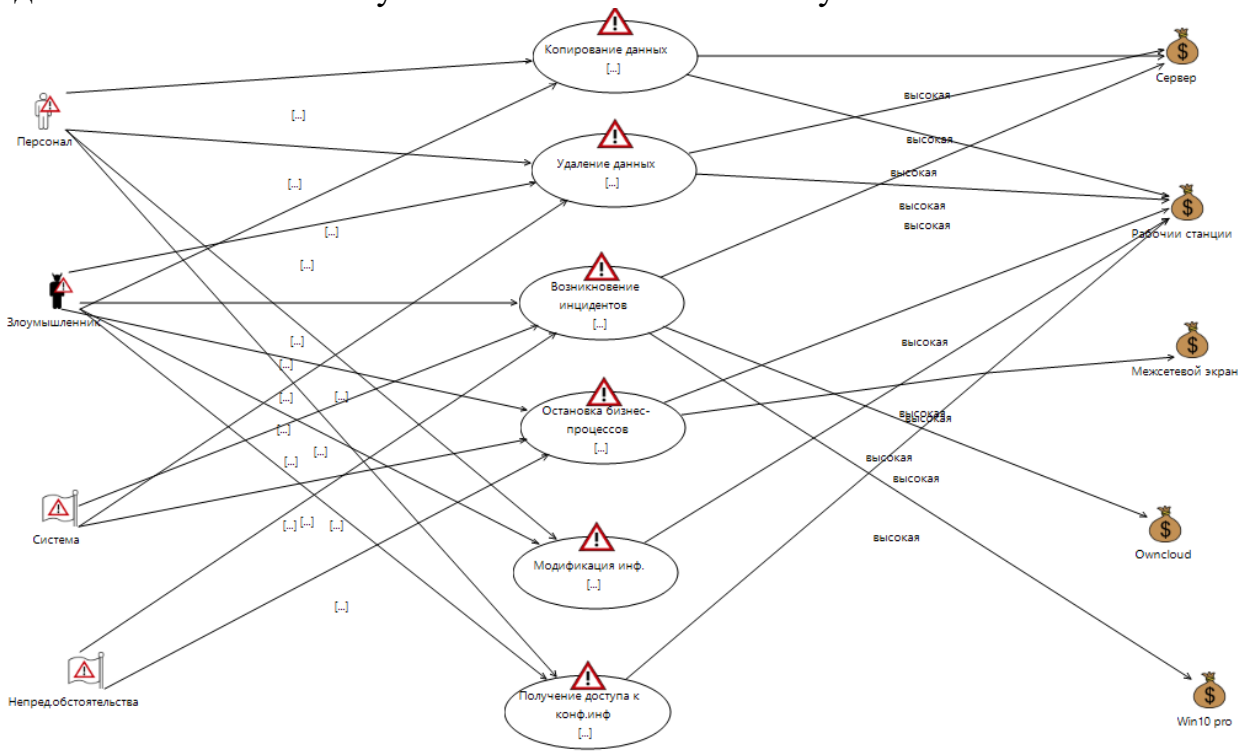
5.4 сурет – Қауіпті жүзеге асыру салдарының сипаттамасы бар тәуекелдер диаграммасы

5.3 суреттегі диаграмманы қолданғаннан кейін, қауіп-қатер үшін қорғаныс шараларын қосамыз.



5.5 сурет – Қарсы әрекет етуді қосқаннан кейінгі қауіптер диаграммасы

Бұл диаграммада қорғаныс шараларын қосқан кезде де қалуы мүмкін тәуекелдерді көрсетеді. Жүйелердің толық мониторингі кезінде қауіптердің пайда болуы азайтылуы тиіс.



5.6 сурет – Қолайсыз тәуекелдер диаграммасы

Бұл бөлімде біз жүйенің осалдығын анықтау және жою мақсатында тәуекелдердің есебін жүргіздік. Есептеу ISO27005 стандартына негізделген екі параметр бойынша жүргізілді. Нәтижесінде біз ақпараттық жүйенің ағымдағы жағдайын көрдік. Бұдан әрі біз қорғаудағы барлық кемшіліктерді көрдік және қорғау құралдарын енгізгенге дейін есептелген тәуекелдерді азайту үшін барлық қорғаныс құралдарын енгіздік. Содан кейін біз тәуекелдерді сол әдіс бойынша қорғау құралдарымен қайта есептеу жасадық. Есептеу нәтижесінде біз тәуекелдердің үш есе төмендеуін айқын көре аламыз және осының арқасында осы есептеу әдісі өте пайдалы екенін растай аламыз, өйткені бизнес үшін шығындардың айтарлықтай азаюына ықпал етеді. Екінші бөлімде біз CORAS арқылы талдау жасадық. Бағдарламада ақпаратты неғұрлым көрнекі ұсыну үшін UML-диаграммалар және жалпы активтер схемалары, осалдықтар, қауіп-қатерлер ұғымы жұмыс барысында жүргізілген қарсы шаралар салынды.

Қорытынды

Дипломдық жұмыста бұлтты сервистер даму бағыты мен жұмыс істеу сипаттамаларына салыстырмалы талдау жасалынды және қауіпсіздік сұрақтары талқыланды. Осыған негізделе отандық IaaS сервистерінің салыстырмалы сипаттамасы жүргізілді. Салыстыру кезінде отандық бұлтты нарық даму барысында екендігін анықталды және отандық қызмет берушілер бұлтты қызметтерге деген сұраныстың тек 27% - ын ғана қанағаттандырады. Осымен қатар қәзіргі уақытта отандық нарықта «Қазақтелеком» провайдерінің үлесі 50%-дан артық екендігі белгілі болды. Дегенімен отандық нарықтың даму мүмкіндіктері өте зор, себебі, 5G, IoT, Big Data, VR, AI және Smart City секілді қызметтерді енгізу үстінде. Қауіпсіздік жағынан Қазақстанда бұлтты сервистер даму үстінде және ірі провайдерлерде жоғары деңгейде ұйымдастырылған.

Бұлттық технологиялардың танымалдығының артуына байланысты зиянкестер ұйымдардың бұлттық инфрақұрылымына енудің түрлі тәсілдерін белсенді әзірлейді және қолданады, сондықтан желілік қауіпсіздікке үйреншікті тәсілдер белгіленген талаптарды қанағаттандырмайды. Бұлтты құру ерекшеліктеріне назар аудара отырып (Интернет желісінен қол жетімділік, бөлінген байланыс арналарын пайдаланудың мүмкін еместігі, белгілі бір жағдайларда — трафикті шифрлаудың мүмкін еместігі және сонымен қатар қатынау нүктелерінің көп саны), оны қорғауға мұқият қарау қажет.

Бұлттық қызметтерді бүкіл әлем бойынша 90%-дан астам жүйелер пайдаланады. Бұлттар ақпараттық технологияларға ұзақ уақытқа келді. Жалпы әлемдік бұлтты технологиялар даму бағыты белгіленіп өзекті мәселе қауіпсіздік болып тұр. Ал, негізгі қорғау жүйелерінің құрылуы бұлт және құрылғыларда болуы тиіс себебі, бұл бізге жылдам түрде бұлттың дамуына көмек береді және екі жақты қауіпсіздікті әлдеқайда арттырады.

Осы өзгерістердің табысты болуы үшін қауіпсіздік мәселелері кедергі емес, тек қауіпсіз бұлтты технологияларға ауысуға себеп болуы тиіс. Бұлтқа арналған құрылғылардан барлық жол бойы қорғауды қамтамасыз ету бұлт ортасын қорғау оларды қалыптастыру кезеңінен немесе жұмыс жүктемелерін автоматты түрде өрістету процесінде қорғау құралдарын орнату арқылы немесе жаңа бұлт қосымшасына бірінші рет қол жеткізу кезінде мәліметтердің жоғалуын болдырмау саясатын пайдалану арқылы қамтамасыз етілетінін білдіреді.

Әдебиеттер тізімі

1. Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Software & Systems Программные продукты и системы // Облачные технологии: основные модели, приложения, концепции и тенденци и развития.
2. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing.Облачные вычисления.
3. Богомолов И. В., Алексиянц А. В., Борисенко О. Д. и др. (2016) Проблемы масштабируемости облачных сред и поиск причин деградации центрального сервиса идентификации Openstack Keystone.
4. Монахов Д.Н., Монахов Н.В., Прончев Г.Б., Кузьменков Д.А. ―Облачные Технологии. Теория и практикакнига‖ МАКС Пресс Москва, МГУ, 2013 г. – С. 128
5. Грейс Уокер, "Основы облачных вычислений", Справочник IBM.
6. Pierre Audoin Consultants [Электронныйресурс] /https://www.pac-online.com/
7. Официальный сайт компании Apache CloudStack™ [Электронныйресурс] / http://cloudstack.apache.org
8. Официальный сайт компании Eucalyptus [Электронныйресурс] / https://www.eucalyptus.com
9. Официальный сайт компании Vmware / http://www.vmware.com/
10. Официальный сайт компании Openstack / http://www.openstack.org/
11. Официальный сайт компании Amazon / https://www.amazon.com
12. Официальный сайт компании Tucha [Электронныйресурс] / http://tucha.ua/
13. Официальный сайт компании Volia [Электронныйресурс] / http://cloud.volia.com/
14. Методологии управления ИТ-рисками. // www.osp.ru URL: https://www.osp.ru/os/2006/08/3584582/
15. Bjorn, A.G. (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security (**www.nr.no/coras**)
16. http://анализ-риска.рф/content/ponyatie-riska
17. https://www.terra-security.ru/blog/analiz-skud-kak-proverit-sistemu-kontrolya-i-upravleniya-dostupom-na-effektivnost
18. Жандаулетова, Ф. Р. Охрана труда: учебник для вузов / Ф.Р. Жандаулетова, Т.Е. Хакимжанов, Т.С. Санатова; МОН РК, НАО АУЭС. - Алматы : АУЭС, 2019. - 399 с.
19. Гигиенические требования к микроклимату производственных помещений: Санитарные правила и нормы СанПиН 2.2.4.548-96.—М.; Информационно-издательский центр Минздрава России, 2001. —20 с
20. ҚР ҚНжЕ 4.02-42-2006. «Жылыту, желдету және ауа баптау» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2007.

21. ҚР ҚНжЕ 2.04-05-2002 – «Жасанды және табиғи жарықтандыру» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002.

22. ҚР ҚНжЕ 2.02-05-2009 – «Ғимараттар мен имараттардың өрт қауіпсіздігі» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2010.

23. ҚР ҚНжЕ 2.04-01-2001. «Құрылыстық климатология» - Сәулет, қала құрылысы және құрылыс саласындағы мемлекеттік нормативтер, Астана, 2002.

24. Абикенова А.А., Санатова Т.С. Безопасность жизнедеятельности. Методические указания к выполнению раздела «Пожарная профилактика» в выпускных работах для всех специальностей. Бакалавриат - Алматы: АИЭС, 2009. - 32 с.

25. Ж.С. Абдимуратов. Охрана труда. Методические указания к выполнению расчетно-графических работ для студентов - бакалавров специальности 5В071800 - «Электроэнергетика» - Алматы: АУЭС, 2013 - 22с.

26. ҚР СНиП 2.04.-05.2002 Табиғи және жасанды жарық. Құрылыс, қала құрылысы және архитектура саласындағы мемлекеттік нормативтері.