УДК 004.056.5 https://doi.org/10.51301/vest.su.2021.i2.25

Ш.А. Абдалы*
әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
*e-mail: shyngys.abdaly@gmail.com

БҰЛТТЫ ЕСЕПТЕУЛЕР ЖӘНЕ БҰЛТТАҒЫ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ НЕГІЗДЕРІ

Андатпа. Мақалада бұлтты есептеулер мен оның виртуалды технологиялар негізінде ұсынылатын қызметтерге шолу жасалған. Технологиялық прогресс адам өмірінің барлық салаларына әсер етуде. Ақпараттық технологиялар әлемінде ай сайын бірнеше мың қызметтер мен жобалар жасалуда. Көптеген компаниялар бұлтты қызметтерге жергілікті жобалардың жұмысын жақсарту, компанияның архитектурасы мен инфрақұрылымын жақсарту, бюджет пен уақытты үнемдеу мақсатында көшуде. Бұлтты есептеулерге жаппай көшу, бұл бұлтты қоймалардағы пайдаланушылардың жеке деректерінің жүз пайыз қауіпсіздігін қамтамасыз етеді деген қате ой тудырады. Әрбір пайдаланушының жеке ақпараты құпия дерек болып табылады, сондықтан бұлтты жүйелер пайдаланушы деректерінің тұтастығы мен сенімді қорғалуын қамтамасыз етуі қажет. Бұл мақалада бұлтты есептеулердегі қауіпсіздік шараларына талдау жүргізіледі.

Негізгі сөздер: бұлтты есептеулер, интернет, инфрақұрылым, сервистер, IaaS, PaaS, SaaS.

Кіріспе. Қолданушылар жеке ақпараттарын жедел, автоматты түрде қашықтықта орналасқан деректер қоймасында сақтай алады. Бұл дегеніміз адамдардың бұлтты технологиялармен әрдайым өзара әрекеттесу процесінде екендігін көрсетеді. Бірақ бұлтты есептеулер ол тек ақпараттарды сақтайтын деректер қоймасы ғана емес, бұлтты есептеулер бізге кең ауқымды сервистер жүйесін ұсынады. Басқаша айтқанда біз бұлтты есептеулер ұсынатын сервистермен қолданамыз. Бұл сервистерге мысал ретінде электронды пошта, мобильді қосымшаларды ұсынатын онлайн дүкендер, сайтты орналастыратын бұлтты хостингтер және де басқаларын келтіруге болады. Бұлтты технологиялар термині қолданысқа енген кезден бастап, ақпараттық технологиялар қауымдастығында қызу талқыланатын ең басты тақырыптардың бірі ондағы қауіпсіздікті қамтамасыз ету болды. Бұлтты есептеулерге жаппай көшу, бұл бұлтты қоймалардағы пайдаланушылардың жеке деректерінің жүз пайыз қауіпсіздігін қамтамасыз етеді деген елес тудырады. Әрбір пайдаланушының жеке ақпараты құпия дерек болып табылады, сондықтан бұлтты жүйелер пайдаланушы деректерінің тұтастығы мен сенімді қорғалуын қамтамасыз етуі қажет.

Бұлтты есептеулерге шолу. Бұлтты есептеулерге анықтама берсек, бұл интернет желісі арқылы ыңғайлы есептеу қызметтерін ұсыну [1]. Бұлтты есептеулердің негізгі мүмкіншіліктері кәсіпорындардың жұмысында айқын көрінеді. Кәсіпорындар үшін қуаты мықты серверді сатып алу, компьютердегі бағдарламалық қамтамасыз етуді орнатуға, жаңартуға қаражат жұмсау қажеттілігі жоқ. Кәсіпорындар тек қолданатын сервистері үшін ғана қаражат жұмсайды. Үлкен деректер қорымен жұмыс істеуге, онда ақпараттарды өңдеуге, саралауға болады. Сонымен қатар кәсіпорын қызметкерлерінің жұмысына қажетті құралдар веб сервис арқылы автоматты түрде ұсынылады. Кәсіпорын қызметкері физикалық жұмыс орнына байланбай, интернетке қосылған кез келген құрылғыдан жұмыс істей алады. Орта және кіші кәсіпорындары үшін уақыт пен қаражат маңыздылығы зор және бұлтты есептеулер кәсепорындарға осы ресурстарды үнемдеуге мүмкіншілік туғызады. Бұлтты есептеулерді ұсынатын көптеген провайдерлер бар, солардың бірі Microsoft Azure. Бұл компания осы нарықта монополистер қатарына жатады. Microsoft Azure-дың сайтында жазылған ақпаратқа сүйенетін болсақ, бұлтты есептеулердегі 6 маңызды артықшылықтары аталған, олар шығындарды азайту, жылдамдық, ғаламдық масштаб, өнімділік, сенімділік, қауіпсіздік.

1. Бұлтты есептеулер жабдықтар мен бағдарламалық жасақтаманы сатып алуға, жергілікті деректер орталықтарын орнатуға және пайдалануға күрделі шығындардан аулақ болуға мүмкіндік береді.

2. Бұлтты есептеулер қызметтерінің көпшілігі өзіне-өзі қызмет көрсету режимінде және сұраныс бойынша ұсынылады, сондықтан есептеу ресурстарының үлкен көлемін бірнеше минут ішінде дайындауға болады, әдетте тінтуір түймесін бірнеше рет басу арқылы. Бұл компанияларға икемділік береді және тұрақты жүктеуді жоспарлаудан арылуға мүмкіндік береді.

3. Бұлтты есептеулер қызметтерінің артықшылықтары серпімді масштабтау мүмкіндігін қамтиды. Бұл дегеніміз ақпараттық технологиялар ресурстарының тек қажетті көлемін бөлуді білдіреді. Мысалы, өңдеу қуатын, сақтау көлемін немесе өткізу қабілетін арттыру немесе азайту.

4. Жергілікті деректер орталықтары әдетте көптеген тіректер мен серверлерді, сонымен қатар жабдықты орнатуды, бағдарламалық жасақтаманы жаңартуды және уақытты қажет ететін басқа да жұмыстарды талап етеді. Бұлтты есептеулер осы тапсырмалардың көпшілігін болдырмайды.

5. Бұлтты есептеулер деректердің сақтық көшірмесін жасауды, апаттық жағдайларды қалпына келтіруді және бизнес-процестердің үздіксіздігін жеңілдетеді және арзанырақ етеді.

6. Бұлтты есесптеулерді ұсынатын провайдерлер деректерді, қосымшалар мен инфрақұрылымды ықтимал қауіптерден қорғауға көмектесетін, қауіпсіздік деңгейін арттыратын көптеген саясаттар, технологиялар және басқару құралдарын ұсынады.

Бұлтты инфрақұрылым келесі орналастыру модельдерінің біреуінде жұмыс істей алады: қоғамдық, жеке, қауымдастық және гибридті [2]. Қоғамдық бұлт көптеген компаниялар мен сервистер жұмыс жасайтын ақпараттық технологиялар инфрақұрылымы. Қоғамдық бұлттың қолданушылары бұлтты есептеулерді басқару және қадағалау мүмкіншілігіне ие емес. Қолданушылар тек провайдер ұсынатын қызметтермен жұмыс жасай алады. Қоғамдық бұлт инфрақұрылымына мысал ретінде веб түріндегі Microsoft Office бағдарламасын, Google Docs секілді сервистерді келтіруге болады. Жеке бұлт тек бір ғана кәсіпорнына берілетін бұлтты инфрақұрылым. Мұнда кәсіпорындар бұлтты есептеулерді басқару мүмкіншілігіне ие болады. Көбінде жеке бұлттар кәсіпорын аумағында орналастырылады және оның қызметіне сол кәсіпорын жұмысшылары жауапты болады. Қауымдастық бұлт бірнеше кәсіпорнына берілген бұлтты инфарқұрылым түрі. Гибридті бұлт жеке және қоғамды бұлттарды қамтиды. Көбінде кәсіпорындар жеке бұлттармен уақытша жұмыс жасайтын болса, осы гибридті бұлтты инфрақұрылымға көшуді ұйғарады. Себебі жеке бұлтты есептеулерді қолдануға ауқымды қаражат жұмсалады.

Виртуалды технологиялар негізінде ұсынылатын қызметтер бірнеше топқа бөлінеді. Бұлтты есептеулерде қызметтер модельдері көп, бірақ қолдану жиілігі мен маңыздылығына қарай үлкен 3 топқа жіктейді, олар IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) [3].

IaaS (Инфрақұрылым қызмет ретінде) – бұл клиенттің кез келген қосымша мен бағдарламалық қамтамасыз етуді орната алатын есептеу ресурстарын жалға алу. Операциялық жүйелер мен қосымшалар деңгейіндегі параметрлерді клиенттің өзі жүзеге асырады, ал сервер мен желілік жабдықты басқарудың барлық мәселелерін провайдер шешеді.

PaaS (Платформа қызмет ретінде) – клиенттер деректерді енгізу,нәтиже алу және провайдер мүмкіндік беретін дәрежеде тиісті платформаны орнату үшін бағдарламалық жасақтамамен өзара әрекеттесе алады. Тапсырыс беруші бағдарламалық жасақтамаға немесе қосымшаларды әзірлеуге жауапты емес, тек платформамен өзара әрекеттескені үшін жауапты. Қызмет көрсетуші техникалық қызмет көрсету, қызметтің барлық пайдалану аспектілеріне

және өнімнің өмірлік циклін басқаруға міндетті. Көп жағдайда PaaS шешімін жеткізуші әзірлеуші болып табылады, ол клиентке толық шешім ұсынады. Google да осы жүйеде PaaS провайдері ретінде әрекет етеді, өйткені ол өз клиенттеріне осы қызмет моделінің бөлігі ретінде көптеген веб-қызмет қосымшаларын ұсынады. Google карталары, Google Earth, пошта және басқа да көптеген ұсыныстарды мысал ретінде келтіруге болады.

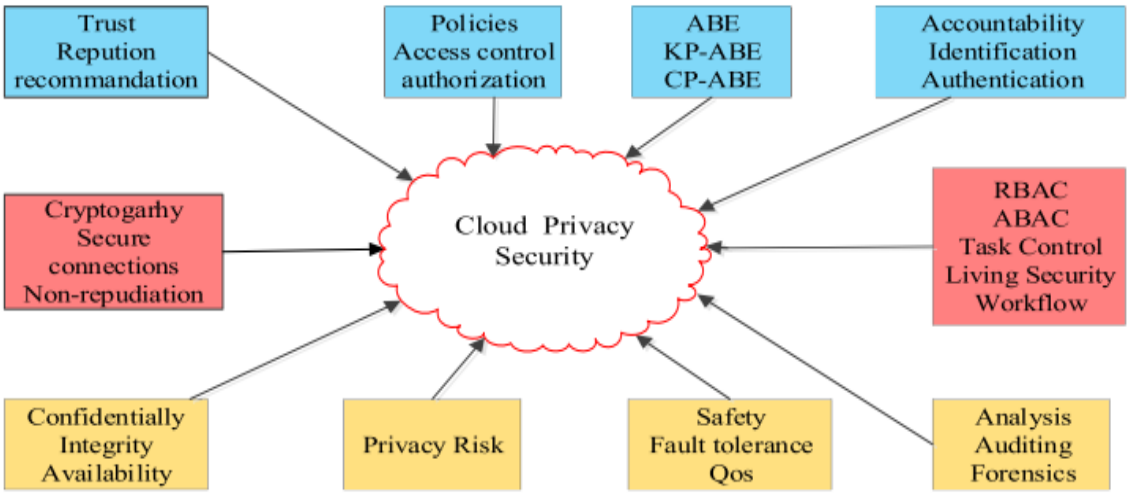
SaaS (Бағдарламалық жасақтама қызмет ретінде) – бұнда провайдер есептеу жабдықтары мен бағдарламалық қамтамасыздандыру, сонымен қатар кешенді қызмет ретінде шешімдерді ұсынады. SaaS бұлтты есептеу қызметінің ең толық моделі болып саналады. Қызмет ретінде бағдарламалық жасақтаманы хостингте орналастырылған бағдарламалық жасақтама ретінде қысқаша сипаттауға болады. Сервис бүкіл әлем бойынша интернет арқылы, көбінесе браузерде қолжетімді болады.

Бұлтты қызметтер мен шешімдер саны (SaaS, Paas, IaaS) өсуді жалғастырады. Бұл тұжырымның келесі мақалада сандар арқылы ашық көрсетілген [4]. Bain & Company мәліметтері бойынша, 2020 жылға қарай SaaS – қа жазылудың бірлескен жылдық өсу қарқыны 18% - ға артады. PaaS 2016 жылы 32% -дан 2019 жылы 56% -ға дейін өседі, бұл бұлтты платформалардың ең қарқынды дамып келе жатқан секторына айналады, деп хабарлайды KPMG. Ал IaaS нарығы 2020 жылға қарай бүкіл әлем бойынша 72,4 миллиард долларға жетеді деп жазалы Gartner.

Бұлтты технологияларды қолдану жайлы PWC компаниясы жүргізген аналитакалық зерттеудің нәтижелеін келтіре кетуге болады [5]. Бұл зерттеуде зерттеуге қатысушылардан, яғни компания өкілдерінен неліктен бұлтты технологияларға өтуден тайынады деген сұрақтар қойылған. Зерттеуге қатысушылардың 36% жеке деректердің бөтен қолдарға өтіп кетуінен, 45% заянды бағдарламалық вирустардың енуінен, 27% есептік жазбаның бұзылуынан қорқу салдарынан бұлтты технологияларға асыға өтуден тартынатындығын көрсетеді. Тағы бір сауалнамада бұлтты технологияларға төнетін ең үлкен қауіп қандай деген сұраққа, зерттеі қатысушыларының 45% рұқсатсыз кіру, 38% бұлтты сервистерді қате орнату, 36% жеке деректердің ұрлануы, 31% провайдер тарапынан қорғау шараларының жеткіліксіздігін көрсетеді. Осы пайыздық қатынасқа анализ жүргізсек, қолданушылардың бұлтты технологияларды жаппай қолданудан ең үлкен қаупі, ол жеке деректердің қауіпсіздік мәселесі екендігіне көз жеткізуге болады.

Бұлтты есептеулердегі қауіпсіздікті қамтамасыз ету. Бұлтты есептеулер деректерді өңдеу орталығында немесе серверде орналастырылады. Деректерді өңдеу орталықтары бұл серверлер мен интернетке қосылған желілік жабдықтамалар сақталатын орын. Деректерді өңдеу орталықтары әрдайым электр қуатына қосылу және салқындату жүйесімен жабдықталған болады, сонымен қатар онда түрлі қауіпсіздік шаралары қарастырылған. Сервер дегеніміз ақпараттық технологиялар инфрақұрылымының жұмысын қамтамасыз ететін қосымшалар мен қызметтердің жұмысы үшін қолданылатын мамандандырылған компьютер. Бұлтты технологияларды ұсынатын ірі провайдерлерде өзінің деректерді өңдеу орталықтары бар. Ал кіші провайдерлер бұлтты есептеулерді серверде орналастырады. Бұл дегеніміз сервердің физикалық шабуылға, табиғи апаттарға осал болатындығын көрсетеді [6]. Сондықтан бұлтты технологияларды ұсынатын провайдерді таңдағанда осы фактрге мән берген жөн.

Пайдаланушының жеке деректері құпия болып табылады және бұлтты есептеулерде де осы қағида талаптары орындалуы қажет. Деректерді сақтау, виртуалдандыру, үлкен деректер және тағы да басқа технологиялар даму аясында адамдар өздерінің ақпараттарының құпия сақталатындығына алаңдайды, бұлтты есептеулердегі қауіптер көрсетілген (1-сурет) [7].



1-сурет. Бұлтты есептеулердегі қауіптер мен онымен байланысты технологиялар

Құпиялылық пен қауіпсіздік бұлтты есептеулердің негізгі алғышарттары, деректер ресурстарына қауіпсіз және тиімді қол жеткізуді басқару бұлтты есептеулердегі басты мәселе болып табылады. Бұлтты есептеулерде қатынасты басқарудың (access control) бірнеше маңызды технологиялары бар. Олар DAC (discretionary access control), MAC (mandatory access control), RBAC (role based access con- trol), TBAC (task based access control), UCON (usage con- trol), ABAC (attribute based access control) және олардың өнімділігі Кесте 1-де салыстырылған.

Кесте 1. **Қатынасты басқару модельдерінің негізгі түрлері мен олардың өзара салыстырылуы**

Қатынасты басқару модельдері/ қасиеттері	RBAC	TBAC	ABAC	UCON	MAC	DAC
Қауіпсіздігі	X	X	X	√	√	X
Құпиялылығы	X	X	X	X	√	√
Басқару икемділігі	√	√	√	√	X	√
Минималды артықшылығы	√	√	√	√	√	X
Міндеттерді бөлу	√	√	√	X	√	X
Сипаттау қабілеті	√	√	√	X	√	√
Ұсақтылығы	X	√	√	√	√	√
Шектеу сипаттамасы	√	X	√	√	√	X
Динамика	√	√	√	√	X	√
Үйлесімділігі	√	X	√	√	X	√
Кеңейтілуі	X	√	√	√	X	√
Басқару жеңілдігі	√	X	X	X	√	X
Модельдеу жеңілдігі	√	X	√	√	X	√

Желілік қауіпсіздікте ақпараттың құпиялығы мен деректердің тұтастығын міндетті түрде қамтамасыз ететін негізгі кілт ол, заңды пайдаланушыларға әртүрлі деректерге қол жеткізуге өкілеттік бере алатын қатынасты басқарудағы ережелер мен рәсімдер тобы. Дәстүрлі желілік ортамен салыстырғанда бұлтты ортада қатынасты басқаруды басқару технологиясы маңыздырақ. Бұлтты есептеулерде қауіпсіздікті қамтамасыз ету үшін сервис провайдерлері арасында өзара аутентификация және қатынасты басқару амалдары және деректер қауіпсіздігін қамтамасыз етудің тиісті механизмдері қажет, сонымен қатар бұлтты есептеулер клиенттері үшінші тарап арналары бойынша шабуылдарын болдырмау керек. IaaS моделінде

бұлтты сервис провайдерлері жалғыз хостта бірнеше тұтынушыларға арнап көптеген виртуалды машиналарды құрады. Бұл кіріс пен ресурстарды пайдалануды барынша көбейтумен қатар, жаңа осалдылықты тудырады [8]. Осы ретте үшінші тарап арналары бойынша шабуылдар қаупі туындайды. Осы шабуылдың алдын алу үшін виртуалды машиналарды тарату стратегиясын жүзеге асыру қажет.

Екі қабатты шифрлау - бұлтты есептеулердегі деректерді қорғаудың жақсы тәсілдерінің бірі. Бұл мақалада AES жене Rabbit алгоритмдері қолданып екі қабатты шифрлау арқылы деректерді қорғау моделі ұсынылады [8]. Алдымен Rabbit алгоритмімен шифрлау жүргізіледі, кейіннен сәйкесінше AES алгоритмі орындалады. Rabbit алгоритмі ағынды шифрлау түріне жатады және бағдарламалық жасақтаманы іске асыруда жоғары өнімділікке арналған. Бұл алгоритм генерация негізінде алынған 64 немесе 128 бит блок негізінде жұмыс істейді. Ал AES алгоритмінің таңдалуы оның итеративті негізде жұмыс істеуінде, ол өз кезегінде DES алгоритмі негізіндегі Фейштель кестесінен күрделі, сонымен қатар 128/192/256-битті кілттерден тұрады.

Пайдаланушы файлдары бұлт қоймаларына алғашқы шифрлаусыз, яғни бастапқы түрінде жібереді. Бұл жағдайда бұлтты ортада жеке ақпаратты сақтау қауіпті болады, өйткені бұлтты инфрақұрылымды ұсынатын провайдер осы деректерді өңдеуге мүмкіндік алады. Бұған жол бермеу үшін барлық жеке деректерді бұлтқа жіберместен бұрын шифрлау керек. Бірақ бұл жағдайда бұлтты есептеу шифрланған деректерде еркін операцияларды орындай алмайды. Бұл проблеманы криптографиялық алгоритмдер арқылы шешуге болады. Осындай шешімге гомоморфты шифрлеу арқылы қол жеткізуге болады [10]. Гомоморфты шифрлеу жеке кілтті білмей, шифрланған ақпаратқа есептеу жүргізуге мүмкіншілік тудырады. Гомоморфты шифрлеуді математикалық түрде HE (A) және HE (B), HE (C (A, B)) операциясын орындайды деп көрсетуге болады, мұндағы C: қосу, көбейту немесе X-or операторланың бірі бола алады.

Қорытынды. Бұлтты есептеулердің қазіргі уақытта қарқынды дамып жатқан ғылыс саласы екендігіне көз жеткіздік. Бұлтты есептеулерге бұлтты есептеулер мен оның виртуалды технологиялар негізінде ұсынылатын қызметтерге, бұлтты инфрақұрылымда деректерді қорғау үшін қолданылатын белгілі криптографиялық алгоритмдерге шолу жасалынды. Бұлттағы қауіпсіздікті қамтамасыз ету негіздері айқындалды.Бұлтты есептеулерде қатынасты басқарудың бірнеше маңызды түрлері атап көрсетілді және өзара салыстырулар жүргізілді. Екі қабатты шифрлеу, гомоморфты шифрлерге қысқаша шолу жасалынды.

ӘДЕБИЕТТЕР

[1] De Donno M., Tange K., Dragoni N. Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog // IEEE Access. IEEE, 2019. Vol. 7. P. 150936–150948.

[2] Patel J., Suthar F., Khanna S.V.O. A Critical Analysis on Encryption Techniques used for Data Security in Cloud Computing and IOT (Internet of Things) based Smart cloud storage System : A Survey // IJSRNSC. 2019. Vol.7, № 2. P. 21–25.

[3] Курбанов З.М. Облачные технологии: обзор и применение // Вестник науки и образования. 2019. Vol. 4, № 58. P. 55–60.

[4] Ashok A. Four trends in cloud computing CIOs should prepare for in 2019 // Forbes Community Voice. 2018.P. 4.

[5] Виталий Соколов, Михаил Курзин П.Н. Исследование PwC « Страх облаков » // pwc. 2020.

[6] Вишняков А.С. et al. Обеспечение защиты данных, представленных в облачных сервисах // Вестник науки и образования. 2019. Vol. 11, № 65. P. 22–29.

[7] Sun P.J. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions // IEEE Access. 2019. Vol. 7. P. 147420–147452.

[8] Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Ligang Cong J.L., Yang H. Security Strategy for Virtual Machine Allocation in Cloud Computing // Procedia Comput. Sci. Elsevier B.V., 2019. Vol. 147. P. 140–144.

[9] Taiwade M.Hi. Dual Layer Data Security in Cloud Computing // Int. J. Res. Appl. Sci. Eng. Technol. 2019. Vol. 7, № 10. P. 170–173.

[10] Amruta Patil, Apurva Kirve, Sayali Nandeshwar, Swati Ture N.R.S. Homomorphic Encryption Security for Cloud Computing // Int. Res. J. Eng. Technol. 2020. Vol. 7, № 5. P. 1–4.

REFERENCES

[1] De Donno M., Tange K., Dragoni N. Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog // IEEE Access. IEEE, 2019. Vol. 7. P. 150936–150948.

[2] Patel J., Suthar F., Khanna S.V.O. A Critical Analysis on Encryption Techniques used for Data Security in Cloud Computing and IOT (Internet of Things) based Smart cloud storage System : A Survey // IJSRNSC. 2019. Vol.7, № 2. P. 21–25.

[3] Kurbanov Z.M. Cloud technologies: overview and application // Vestnik nauki i obrazovaniya [Bulletin of science and education]. 2019. Vol. 4, № 58. P. 55–60.

[4] Ashok A. Four trends in cloud computing CIOs should prepare for in 2019 // Forbes Community Voice. 2018.P. 4.

[5] Vitaly Sokolov, Mikhail Kurzin P.N. Исследование PwC [Reserch of PwC] «Fear of the clouds » // pwc. 2020.

[6] Vishnyakov A.S. et al. Ensuring the protection of data presented in cloud services //
Vestnik nauki i obrazovaniya [Bulletin of science and education]. 2019. Vol. 11, № 65. P. 22–29.

[7] Sun P.J. Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions // IEEE Access. 2019. Vol. 7. P. 147420–147452.

[8] Hefei Jia, Xu Liu, Xiaoqiang Di, Hui Qi, Ligang Cong J.L., Yang H. Security Strategy for Virtual Machine Allocation in Cloud Computing // Procedia Comput. Sci. Elsevier B.V., 2019. Vol. 147. P. 140–144.

[9] Taiwade M.Hi. Dual Layer Data Security in Cloud Computing // Int. J. Res. Appl. Sci. Eng. Technol. 2019. Vol. 7, № 10. P. 170–173.

[10] Amruta Patil, Apurva Kirve, Sayali Nandeshwar, Swati Ture N.R.S. Homomorphic Encryption Security for Cloud Computing // Int. Res. J. Eng. Technol. 2020. Vol. 7, № 5. P. 1–4.

Ш.А. Абдалы*
Казахский национальный университет им.аль-Фараби, Алматы, Казахстан
*e-mail: shyngys.abdaly@gmail.com

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОБЛАКЕ

Аннотация. В статье представлен обзор облачных вычислений и услуг, предоставляемых на основе его виртуальных технологий. Технологический прогресс затронул все области жизни людей. В мире информационных технологий создаются несколько тысяч сервисов и проектов ежемесячно. Все больше компаний переходят на облачные сервисы для улучшения работы локальных проектов, для усовершенствования их архитектуры и инфраструктуры компании, для экономии бюджета и времени. Массовый переход на облачные вычисления создает иллюзию стопроцентной защищенности персональных данных пользователей в облачных хранилищах. Личная информация каждого пользователя является конфиденциальной, поэтому облачные системы должны обеспечить целостность и надежную защиту пользовательских данных. В данной статье проведен анализ мер безопасности в облачных вычислениях.

Ключевые слова: облачные вычисления, интернет, инфраструктура, сервисы, IaaS, PaaS, SaaS.

S.A. Abdaly*
al-Farabi Kazakh National University, Almaty, Kazakhstan
*e-mail: shyngys.abdaly@gmail.com

CLOUD COMPUTING AND THE FOUNDATION OF SECURITY IN THE CLOUD

Abstract. The article provides an overview of cloud computing and services provided on the basis of its virtual technologies. Technological progress has affected all areas of people's lives. In the world of information technology, several thousand services and projects are created every month. More and more companies are switching to cloud services to improve the performance of local projects, to improve their architecture and infrastructure of the company, to save budget and time. The massive transition to cloud computing creates the illusion of one hundred percent security of user’s personal data in cloud storage. Each user's personal information is confidential, so cloud systems must ensure the integrity and reliable protection of user data. This article analyzes security measures in cloud computing.

Keywords: cloud computing, internet, infrastructure, services, IaaS, PaaS, SaaS.