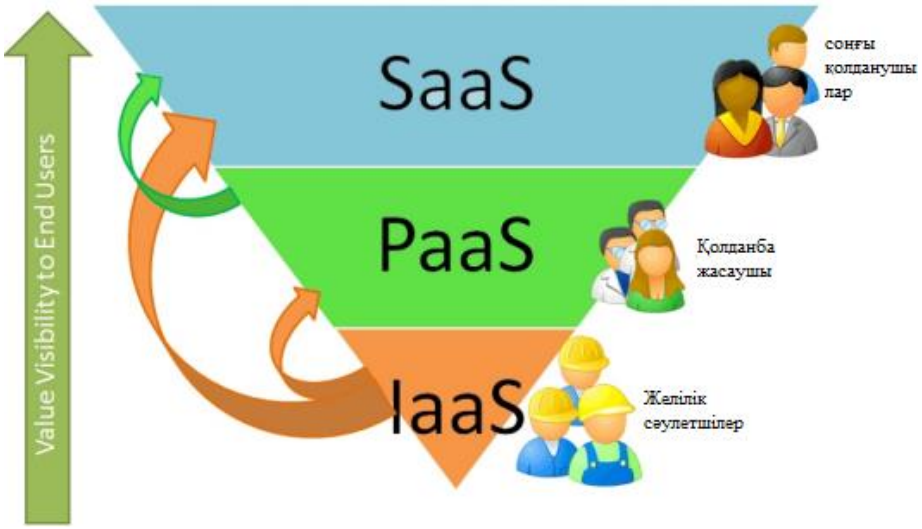
ОӘЖ 004.056

# БҰЛТТЫҚ ЕСЕПТЕУЛЕРДЕГІ ҚАУІПСІЗДІК ШАРАЛАРЫ

**Ғабитова Альбина Бауыржанқызы**
akapon@mail.ru
Л.Н.Гумилев атындағы ЕҰУ ақпараттық технологиялар факультетінің
4-ші курс студенті, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – Сагиндыков Каким Молдабекович

Бұлтты есептеулер конфигурацияланатын ресурстардың, жалпы айтқанда серверлер, сақтау құрылғылары, қосымшалар, желілер мен қызметтердің желіге сұраныс бойынша қол жетімділікті қамтамасыз ету парадигмасы. Басты артықшылығы – IT технологиясы компаниялары үшін уақыт пен шығынды азайту. Қолданушылар бұлтты есептеу қызметтеріндегі бұл ресурстарды бұлтты есептеу ортасында әр түрлі құрылғыда және уақытта, қалаған жерде сұраныс бойынша қосымшалар мен қызметтерді орналастыру және әзірлеу үшін пайдалана алады. Бұлтты есептеу қызмет санаттарына былайша жіктеледі: IaaS (инфрақұрылым қызмет ретінде), PaaS (платформа қызмет ретінде), SaaS (программалық қамтамасыз ету қызмет ретінде), NaaS (желі қызмет ретінде). Қызметтердің осы санаттары қолданушыларға жаңа инфрақұрылым мен ақпараттық-коммуникациялық технологиялардың жаңа жүйелерін оңай бастауға, өзгертуге мүмкіндік береді.

Бұлтты есептеу IT ұйымдардың жұмысын жеңілдетеді және әртүрлі есептеулер мен есептерді қамтамасыз ететін компьютерлер тобын қамтиды. Бұлтты провайдерлер қолданушыларға қашықтан орнатуға және пайдалануға болатын жаңа қосымшаларды тез әзірлеуге, енгізуге мүмкіндік беретін бұлтты ортаға арналған платформаларды (PaaS) немесе программалық жасақтаманы (SaaS) ұсына алады.




Сурет 1. Қызмет көрсету модельдері

Бұлтты есептеулер электрондық түрде деректерді өңдеу және берудің жаңа технологиясы ретінде қазіргі уақытта іс жүзінде әрбір компьютерлік жүйеде қолданылады. Деректерді өңдеу орталығы бір сайтта орналасқан қауіпсіздігімізді арттыру мақсатында қалыптасқан серверлер жиынтығы. Деректер орталығын қорғау физикалық қорғанысты және желіні, ақаулар орын алатын жағдайда төзімділікті білдіреді. Қауіптердің белгілі түрлері, атап айтқанда операциялық жүйенің қосымшаларындағы осалдықтар, зиянды программалық жасақтама, желілік шабуылдар гипервизормен толықтырылды. Қазіргі таңда деректер орталықтарының жұмысы техникалық мәселелер жіне олардың қауіпсіздігі маңызды болғандықтан, оған қатысты мәселелерді жабуды талап етеді. Процессинг орталықтары,

банктер қажетті стандарттарға бағынады, кейінгі орындалуы техникалық шешімдерге байланысты болып келеді. Жүйелерді қолданушы барлық компаниялар виртуалдандыру платформаларындағы қауіпсіздікті күшейтуге өте мұқият қарайды. Қазіргі таңда бизнестің қосымшалары мен маңызды жүйелері қиынға соғады. Осы уақытқа дейін қауіптердің бірнеше түрлері зерттелді және қауіптерге арналған қорғаныс құралдары әзірленді, сонда да бұлтта қолдану әдістерін дамытып, одан әрі бейімдеу керек.

Бұлттарды басқаруды қауіпсіздіктің мәселесі ретінде қарастыруымызға болады. Бұлттың бінеше ресурстарының есептелуіне және бұлт элементтерінің конфигурациясы бұзылмауы, бақыланбайтын виртуалды машиналардың жоқтығына кепілдік берілмеуі және қажетсіз процестер жүрмейді. Жоғары деңгейдегі қауіп түрі бұлттың басқарылуымен байланысты және ол үшін жалпы қорғаныс шаралары жеке-жеке құрылуы керек. Ол үшін тәуекелдерді басқару моделін бұлтты инфрақұрылымдарға қолдану қажет.

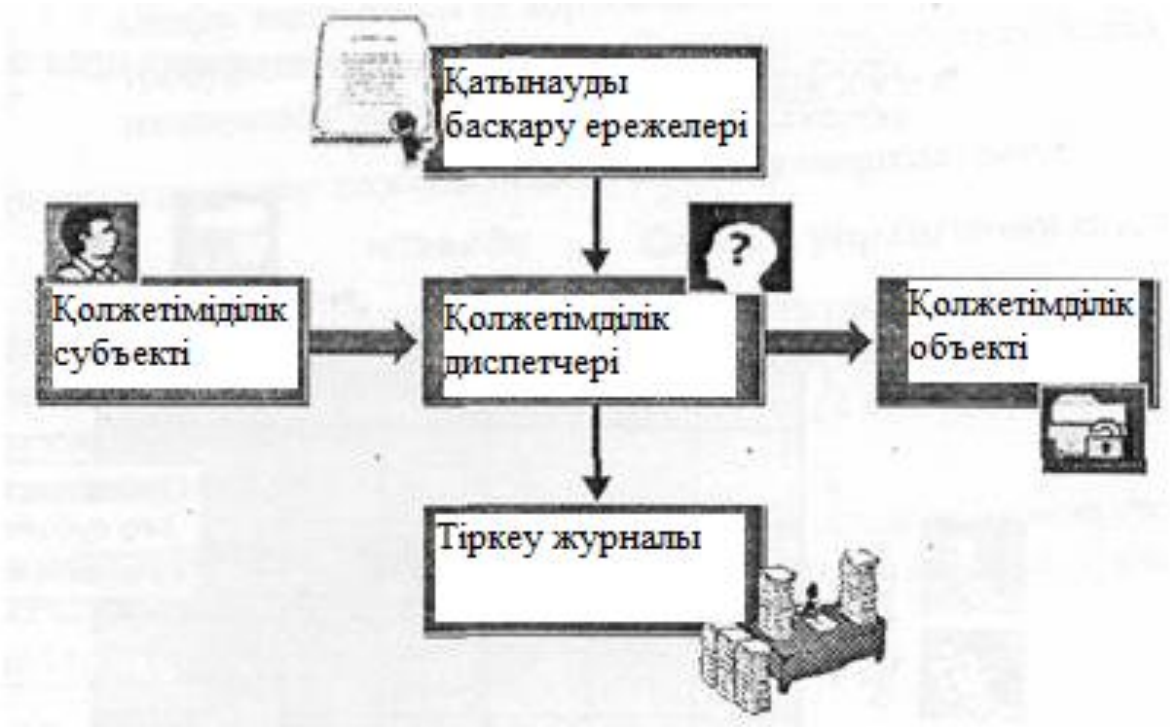
Физикалық қауіпсіздік желілік инфрақұрылым мен серверлерге физикалық қол жетімділікті қатаң бақылауға негізделген. Желілік қауіпсіздіктің физикалықтан айырмашылығы брандмауэрді қамтитын қауіп моделін құру. Деректер орталығының ішкі желілерін бөлу үшін сенім деңгейлерімен жасалған сүзгінің жұмысын брандмауэрді қолдану ретінде қарастырамыз. Интернеттен қол жетімді ішкі желілер, бөлек серверлерден алынған серверлер болуы мүмкін. Виртуалдандыру технологиясы бұлтты есептеуде аса маңызды платформа рөлінде қарастырылады. Бұлтты есептеудегі деректердің қорғалуын және сақталуын қамтамасыз ету үшін негізгі белгілі қауіптерін қарастырамыз.

Бұлтты есептеу қауіпсіздігіне қойылатын талаптар деректерді өңдеу орталығының қауіпсіздік талаптарынан айырмашылығы жоқ. ДӨО виртуализациясы және бұлтты ортаға ауысу жаңа қауіптердің пайда болуына әкеледі. Бұлтты есептеулердің сипаттамалары ретінде есептеу қуатын интернет арқылы басқаруға қол жеткізуді айтуға болады. Инженерлердің серверлерге қол жетімділігі деректер орталықтарында физикалық деңгейде бақыланады, бұлтты ортада интернет көмегімен жұмыс істейді. Бұлтты есептеудің басты критерийлері жүйелік деңгейдегі өзгерістерді қамтамасыз ету және қол жетімділікті шектеу.

Бұлтты есептеу серверлері мен жергілікті серверлер бірдей қосымшалар мен операциялық жүйелерді пайдаланады. Бұлтты жүйелер үшін қашықтан бұзу немесе зиянды бағдарламаны жұқтыру қаупі жоғары, сонымен қатар виртуалды жүйелер үшін де қауіп жоғары. Параллель виртуалды машиналар "шабуыл бетін" арттырады. Интрузияны анықтау және алдын-алу жүйесі бұлтты ортада орналасуына қарамастан, виртуалды машиналар деңгейінде зиянды әрекеттерді анықтай алуы керек.

Виртуалды машина өшірілгенде жұқтыру қаупіне ұшырайды. Желі арқылы виртуалды машиналардың суреттерін сақтауға қол жеткізу жеткілікті. Өшірілген виртуалды машинада қауіпсіздік бағдарламалық жасақтамасын іске қосу мүлдем мүмкін емес. Бұл жағдайда қорғаныс әр виртуалды машинаның ішінде ғана емес, сонымен қатар гипервизор деңгейінде де жүзеге асырылуы керек.

Бұлтты есептеулерді қолданған кезде желінің периметрі бұлдыр. Желінің аз қорғалған бөлігін қорғау қауіпсіздіктің жалпы деңгейін анықтайды. Бұлттағы әртүрлі сенім деңгейлері бар сегменттерді ажырату үшін виртуалды машиналар желілік периметрді виртуалды машинаның өзіне жылжыту арқылы өздерін қорғаумен қамтамасыз етуі керек (Сурет 2). Корпоративтік firewall бұлтты орталарда орналастырылған серверлерге әсер ете алмайтын, IT қауіпсіздік саясатын енгізудің және желі сегменттерін бөлудің негізгі компоненті.




Сурет 2. Кіруді басқару механизмінің схемасы

Модульдік компоненттердің, операциялық жүйелердің, желілік протоколдардың осалдықтары дәстүрлі қауіптер болып табылады, оларды қорғау үшін антивирус, firewall, IPS және осы мәселені шешетін басқа компоненттерді орнату жеткілікті. Виртуализация жағдайында қорғаныс құралдарының тиімді жұмыс істеуі маңызды.

Бұлт элементтерінің функционалды шабуылы бұлт қабаттасуымен, жалпы қауіпсіздік принципімен байланысты. Функционалды шабуылдардан қорғау үшін бұлттың әр бөлігі үшін келесі қорғаныс құралдарын қолдану қажет: прокси үшін DoS шабуылдарынан тиімді қорғаныс, веб-сервер үшін беттердің тұтастығын бақылау, қосымшалар сервері үшін қосымшалар деңгейінің экраны, ДҚБЖ үшін SQL инъекцияларынан қорғау, деректерді сақтау жүйесі үшін дұрыс сақтық көшірмелер, қол жетімділікті бөлу. Жеке-жеке қорғаныс механизмдерінің әрқайсысы жасалады, бірақ олар бұлтты кешенді қорғау үшін жиналмайды, сондықтан бұлтты құру кезінде оларды бір жүйеге біріктіру мәселесін шешу керек.

Клиентке шабуылдар бірнеше пайдаланушылар бұлтқа браузер арқылы қосылады. Мұнда Cross Site Scripting, парольдерді "ұрлау", веб-сессияларды ұстап алу, "ортадағы адам" және тағы басқалар сияқты шабуылдар қарастырылады. Шабуылдың осы түрінен жалғыз қорғаныс ретінде аутентификация және өзара аутентификациясы бар шифрланған қосылымды (SSL) пайдалану.

Гипервизор виртуалды жүйенің негізгі элементтерінің бірі, виртуалды машиналар арасындағы ресурстарды бөлу функциясын атқарады. Гипервизорға шабуыл бір виртуалды машинаның екіншісіне жад пен ресурстарға қол жеткізе алуына әкелуі мүмкін. Сондай-ақ, ол желілік трафикті ұстап, физикалық ресурстарды таңдап, тіпті виртуалды машинаны серверден ығыстыра алады. Қорғаудың стандартты әдістері ретінде виртуалды орталарға арналған мамандандырылған өнімдерді, хост серверлерін Active Directory каталог қызметімен біріктіру, күрделілік пен парольдердің ескіруі саясатын қолдану, сондай-ақ хост серверінің басқару құралдарына қол жеткізу процедураларын стандарттау, виртуализация хостының кіріктірілген брандмауэрін қолдану ұсынылады. Виртуализация серверіне веб-кіру сияқты жиі пайдаланылмайтын қызметтерді өшіруге болады.

Бұлттарда қолданылатын виртуалды машиналардың көпшілігі виртуалды машиналарды құруды, беруді және жоюды сенімді басқара алатын басқару жүйелерінің болуын талап етеді. Басқару жүйесіне араласу кейбір виртуалды машиналарды бұғаттап,

басқаларын алмастыра алатын жасырын виртуалды машиналардың пайда болуына әкелуі мүмкін. Бұлт қауіпсіздігі саласындағы қорғаудың ең тиімді әдістерін Cloud Security Alliance жариялады. Компания жариялаған ақпаратты талдағаннан кейін келесі шешімдер ұсынылды. Шифрлау деректерді қорғаудың ең тиімді әдістерінің бірі. Деректерге қол жеткізуді ұсынатын Провайдер деректер орталығында сақталған клиент ақпаратын шифрлауы керек, сондай-ақ қажет болмаған жағдайда оны біржола жою керек. Тасымалдау кезінде шифрланған деректер аутентификациядан кейін ғана қол жетімді болуы керек. Деректер, тіпті сенімсіз түйіндер арқылы қол жеткізілген жағдайда да, оқылмайды немесе өзгертілмейді. Мұндай технологиялар белгілі, AES, TLS, IPsec алгоритмдері мен сенімді хаттамаларын провайдерлер бұрыннан қолданып келеді.

Бұлттық есептеулердегі аутентификация тиісті заңды немесе жеке тұлғаның бұлттық технология жеткізушісінен берілген деректерге қол жеткізуіне кепілдік береді. Аутентификация бұлтты есептеулерде қамтамасыз етілген кезде, бұлтта сақталған ақпаратқа қол жеткізу кезінде пайдаланушының жеке басын бұлт қызметі провайдеріне дәлелдейді. Провайдердің авторизациялау жүйесімен ашық өзара әрекеттесуі үшін Lightweight Directory access Protocol және Security Assertion Markup Language пайдалану ұсынылады. Бұлттардың көпшілік және жеке түрлері RSA көмегімен аутентификация үшін әр түрлі конструкцияларды пайдаланады. RSA криптожүйесі екі факторлы аутентификация, білім негізінде аутентификация және адаптивті аутентификация сияқты аутентификацияның түрлі үлгілерін қабылдайды. Amazon Web Services виртуалды жеке бұлтты қоса алғанда, веб-сервер мен браузер арасында құпия ақпаратты беруге шоғырланады.Бұлт есептеулерін пайдаланғанда, кейбір сыртқы веб-сайттағы қажетті IP мекенжайларының аутентификациясын қосу үшін прокси серверді баптауға болады. Прокси серверінің URL мекенжайы тек сенімді сайттарға кіруге мүмкіндік береді.

Жеке виртуалды машинаны және виртуалды желіні пайдалану кезінде виртуалды желілер VPN (Virtual Private Network), VLAN (Virtual Local Area Network) және VPLS (Virtual Private Lan Service) сияқты технологияларды қолдана отырып орналастырылуы керек. Көбінесе провайдерлер бірыңғай бағдарламалық ортада код деректерін өзгерту арқылы пайдаланушы деректерін бір-бірінен оқшаулайды. Бұл тәсіл деректерге қол жеткізуге мүмкіндік беретін стандартты емес кодта тесік табу қаупімен байланысты қауіптерге ие. Кодта мүмкін қате болған жағдайда, пайдаланушы басқа деректерді ала алады. Соңғы уақытта мұндай оқиғалар жиі орын алды.

Бұл жұмыстың негізгі мақсаты бұлтты есептеулер туралы түсінік және олардың қауіптері мен қауіпсіздік шараларына тоқталу болды. Осы мақсатта біз бұлттық есептеудің қызмет көрсету модельдері және деректерді қорғау үшін қауіпсіздікті қамтамасыз етудің аса маңызды әдістерін талдадық. Бұлтты есептеу қауіпсіздігінің қауіп-қатерінен қорғаудың сипатталған шешімдерін жүйелік интеграторлар бірнеше рет жеке бұлтты салу жобаларында қолданған. Осы шешімдерді қолданғаннан кейін орын алған оқиғалардың саны айтарлықтай төмендеді.

**Қолданылған әдебиеттер тізімі**


1. Peter M. Mell, Timothy Grance The NIST Definition of Cloud Computing https://www.nist.gov/node/568586
2. Риз Дж. Облачные вычисления. Пер. с англ. — СПб.: БХВ-Петербург, 2017.
3. Грейс Уокер, «Основы облачных вычислений», Справочник IBM, 2016г.
4. Гребнев Е. Облачные сервисы. Взгляд из России – М.: CNews, 2011. – 282
5. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных / Мир Internet. – М.: №2, 2013
6. Бердник А. В. Сравнительный анализ решений по безопасности SaaS сервиса от компании IBM и КРОК // Безопасность информационного пространства: сборник статей. Тюмень, 2012. С. 245-253.