УДК 004.056 **DOI 10.52167/1609-1817-2024-132-3-273-282**

Н.Н. Акатаев, Е.Ж. Айтхожаева, Ж.К. Алимсеитова
Satbayev University, Алматы, Қазақстан
Email: zhuldyz_al@mail.ru

БҰЛТТЫ ИНФРАҚҰРЫЛЫМДАРДЫҢ КИБЕРҚАУІПСІЗДІГІНІҢ МӘСЕЛЕЛЕРІ, АЛДЫҢҒЫ ЗЕРТТЕУЛЕРГЕ ШОЛУ

Аңдатпа. Бұлтты есептеулер пайдаланушылар тарапынан тікелей басқарусыз, талап бойынша деректер қоймалары мен есептеу қуаттары сияқты желілік ресурстарға қол жеткізу құралдарын білдіреді. Қазіргі уақытта компаниялар клиенттерге интернет арқылы бірыңғай платформа ұсынатын мемлекеттік және жеке деректерді өңдеу орталықтарын пайдаланады. Сонымен қатар, бұлтты қызметтерді оңтайландыру үшін есептеулер мен ақпаратты сақтауды соңғы пайдаланушыларға жақындатуға мүмкіндік беретін перифериялық есептеулер (edge computing) белсенді қолданылады. Алайда, бұлтты есептеулерді пайдалануда клиенттер үшін қауіптер мен осалдықтарға байланысты киберқауіпсіздік проблемалары туындайды. Бұл мақалада бұлтты есептеулер мен бұлтты қызметтердің киберқауіпсіздігін қамтамасыз ету мәселелеріне арналған ғылыми жарияланымдарға талдау нәтижелері көрсетілген.

Түйінді сөздер. Бұлтты есептеулер, киберқауіпсіздік, қауіптер, кибершабуылдар, ауытқулар.

Кіріспе.

Бизнес-процестерді оңтайландыру және тиімділікті арттыру үшін бұлтты есептеулер (БЕ) және бұлтты қызметтер (БҚ) кеңінен қолданылады. Қолданыстағы БҚ негізгі түрлеріне бұлтты деректер қоймалары, виртуалды машиналар, бұлтқа негізделген қосымшаларды әзірлеу және орналастыру платформалары және үлкен деректерді өңдеуге және талдауға арналған БҚ кіреді.

Алайда, ықтимал, БҚ-ді пайдалану кеңейген сайын киберқауіпсіздікті (КҚ) қамтамасыз етумен байланысты елеулі проблемалар туындауы мүмкін.

Біріншіден, қаржылық ақпарат пен клиенттердің жеке деректерін қоса алғанда, деректердің көлемі мен сезімталдығының артуымен рұқсатсыз қол жеткізу (РҚЖ), деректерді ұрлау немесе құпиялылықты бұзу қаупі артады. Сонымен қатар, жалпыға қол жетімді бұлттық ресурстарды пайдалану деректерді қорғаудың жеткіліксіздігі, жүйенің дұрыс емес конфигурациясы немесе бұлттық қызметтің осалдығы сияқты осалдықтарға әкелуі мүмкін.

Екіншіден, компаниялар фишинг, DDoS шабуылдары, зиянды бағдарламалар және бұзулар сияқты әртүрлі кибершабуылдарға бейім. Бұлтты қызметтер хакерлердің нысанасына айналуы мүмкін, өйткені олар құнды деректері мен инфрақұрылымына қол жеткізуге мүмкіндік береді. Сонымен қатар, мобильді құрылғылар мен заттар интернетін пайдаланудың артуымен олардың бұлттық қызметтермен интеграциялануына байланысты жаңа осалдықтар мен тәуекелдер пайда болады.

Бұл мақалада компанияларда қолданылатын БҚ КҚ және жалпы БЕ қамтамасыз ету мәселелеріне арналған алдыңғы зерттеулерге талдау жасалды.

Материалдар мен тәсілдер.

[1]-де бұлтты модельдердегі сенімге негізделген БЕ КҚ жүйесін ұйымдастыруды қарастырылады. Яғни, провайдер бұлттық жүйеде деректердің сенімділігін, қауіпсіздігін

және құпиялылығын қамтамасыз етеді. Авторлар таратылған есептеу инфрақұрылымдарында КҚ қамтамасыз етудің тиімді әдісі ретінде сенімге негізделген қол жеткізуді басқару моделін ұсынды. Бұл зерттеуде клиенттердің бұлттық жүйедегі клиенттік және бұлттық активтері олардың сенімін талдау негізінде бағаланады.

[2] бұлтты инфрақұрылымның (БИҚ) КҚ қамтамасыз ету модельдері талданады. Авторлар өз жұмыстарында ақпараттық қызмет объектілерінің БЕ-нің әртүрлі модельдерін қолдануы нәтижесінде пайда болатын таратылған есептеулердің КҚ-нің ерекше мәселелерін қарастырды. Авторлар көрсеткендей, жеке бұлттарды ұйымдар өздерінің ішкі қажеттіліктері үшін пайдаланады. Олар қол жетімділік пен басқаруды қатаң бақылауды қажет етеді. Қоғамдық бұлттарды үшінші тарап провайдерлерімен беріледі және қауіпсіздікке қатысты ашық болмауы мүмкін. Қоғамдық бұлттарда ресурстар әртүрлі клиенттер арасында бөлінуі мүмкін. Бұл қосымша қауіпсіздік шараларын қажет етеді.

[3] авторлар бұлтты жүйелердегі деректердің қауіпсіздігін жақсарту үшін машиналық оқыту (МО) модельдерін қарастырады. Таратылған есептеулерді КҚ қамтамасыз ету тұжырымдамасын авторлар бизнес-қосымшаларды орналастырудың практикалық ортасы ретінде серверлік фермаларды виртуалдандыру контекстінде талқылайды. Авторлардың пікірінше, серверлік фермаларды виртуалдандыру оқшаулау арқылы БЕ қауіпсіздігін қамтамасыз етуге көмектеседі, өйткені фермадағы виртуалды серверлер бір-бірінен оқшауланып, рұқсатсыз қол жеткізуге (РҚЖ) жол бермейді. Сонымен қатар, ферма икемділік пен тиімділікті қамтамасыз ете отырып, жүктемеге байланысты динамикалық түрде масштабтай алады. Виртуалды серверлерде әртүрлі кіруқол жеткізу деңгейлері болуы мүмкін, бұл қауіпсіздікке үлес қосады.

[4] авторлар БЕ үшін қауіптерді жіктеу моделін ұсынады. Жіктеудің ерекшелігі - бұл қауіпсіздік мәселелерін анықтау және шешу үшін МО алгоритмдерінің мүмкіндігіне негізделген. Сонымен қатар, авторлар БЕ үшін тәуекелдерді топтастыру моделін ұсынады. Модель МО алгоритмдеріне негізделген.

Осындай зерттеулер [5] жұмыста жүргізілді. Зерттеу бұлтты қызметтерінің КҚ қамтамасыз етуге бағытталған заманауи тәсілдерді талдауға арналған. Бұлтты есептеу Ақпараттық технологиялар саласындағы ең жылдам дамып келе жатқан салалардың бірі болып табылатындығын ескере отырып, бұлттарда болып жатқан процестердің қауіпсіздігі мен сенімділігін қамтамасыз ету, сондай-ақ клиенттер мен бұлттық қызмет провайдерлерінің өзара әрекеттесу механизмдерін қорғау өте маңызды ғылыми және қолданбалы тапсырма болып табылады. Деректердің жоғалуы және олардың бұзылуы туралы алаңдаушылық кейбір компаниялардың есептеулерін бұлтқа ауыстырғысы келмеуінің бастауында тұр. Автор әртүрлі провайдерлер ұсынатын бұлттық қызметтердің әртүрлілігін талдайды және осы саладағы КҚ қамтамасыз етудің қолданыстағы тәсілдерін салыстырады. Сонымен қатар, әртараптандыру принципіне негізделген жаңа тәсіл ұсынылады. Автордың пікірінше, бұлтты жүйелердің маңызды компоненттерінің сенімділігі мен қауіпсіздігін қамтамасыз ету үшін әртараптандыруды қолдану қажет. Бұл принцип бұлтты есептеу провайдерлерінің, деректер орталығының географиялық орналасуының, бұлттық қызмет көрсету үлгілерінің және бұлттық инфрақұрылымды орналастыру үлгілерінің арнайы комбинациясы арқылы әрбір ресурстың бірегей нұсқасын пайдалану болып табылады.

[6] авторлар бұлттық жүйелерде зиянды бағдарламалық жасақтаманың (БЖ) таралуына байланысты КҚ қауіптерін жою үшін пайдаланылуы мүмкін МО алгоритмдерін зерттейді. Авторлар үш МО алгоритмін қолданатын және зиянды БЖ анықтауға арналған тосқауыл құрылымын ұсынады.

[7, 8] көрсетілгендей, БЕ өсуге айтарлықтай әлеуетіне ие және барған сайын танымал бола бастады. Дегенмен, бірегей сипаттамаларына қарамастан, БЕ әртүрлі

қауіпсіздік қатерлерімен бірге келеді. Қауіп-қатерлерді санаттауды көптеген авторлар, атап айтқанда [5, 8, 9] жұмыстарда жасалды.

Құпиялылық қауіптеріне клиенттік ақпаратына инсайдерлік қауіптер, сондай-ақ сыртқы шабуыл тәуекелдері жатады [10]. [10] біріншіден, клиент ақпараты үшін инсайдерлік тәуекел бұлттық қызмет провайдерінің инсайдері тарапынан клиент туралы ақпаратқа рұқсатсыз немесе заңсыз қол жеткізумен байланысты екенін көрсетеді. Бұл қауіпсіздіктің маңызды мәселесі болып табылады. Екіншіден, сыртқы шабуылдардың қаупі БЕ үшін барған сайын өзекті бола түсуде. Бұл тәуекелге клиенттерге және бұлтқа қосымшаларға бағытталған қашықтағы бағдарламалық немесе аппараттық шабуылдар кіреді [11]. Үшіншіден, ақпараттың ағуы адамның қасақана және/немесе байқаусызда жіберілген қателіктеріне байланысты бұлттық деректер үшін шексіз қауіп болып табылады.

БЕ ұйымдастыру кезіндегі ақпараттың тұтастығына төнетін қатерлер [12, 13] жұмыстарда қарастырылған. Біріншіден, бұл қауіпсіздік параметрлерінің мәндерін, виртуалды машиналарды (ВМ) абайсызда жобалауды және сыртқы клиенттік гипервизорларды дұрыс біріктірмейтін ақпаратты оқшаулау тәуекелі. Екіншіден, бұл клиенттердің қол жетімділігін басқарудың нашарлығы, бұл қол жетімділікті басқарудың тиімсіздігіне байланысты әртүрлі КҚ проблемалары мен қауіптеріне тап болуы мүмкін. Бұл ықтимал шабуылдаушыларға бұлтта орналастырылған ақпараттық активтерге зиян келтіруге мүмкіндік береді [14, 15].

[16, 17] көрсетілгендей, қолжетімділік қауіптеріне, мысалы, БЕ және/немесе БҚ физикалық үзілуі жатады, сонымен қатар бұлттық жүйелерге шабуылдардан кейін қалпына келтірудің тиімсіз стратегияларымен байланысты.

[18, 19, 20, 21] жұмыстарда бұлтты жүйелерге шабуылдың түрлері талданады. [18] желілік шабуыл сценарийлерін талқыланады. Атап айтқанда, авторлар атап өткендей, портты сканерлеу хакерлер үшін айтарлықтай қызығушылық тудырады, өйткені ол сәтті шабуылды бастау туралы ақпарат береді [18]. ВМ негізінде шабуылдарды ұйымдастырудың ерекшеліктері де қарастырылады. Жұмыста бұлтты платформаларда қолданылатын әртүрлі ВМ КҚ әртүрлі мәселелер тудыруы мүмкін екендігі көрсетілген. Мысалы, ВМ кескінінің ішіне орналастырылған зиянды код ВМ жасау кезінде қайталанған жағдайда. Бұлтта жұмыс істейтін қосымшаларға негізделген шабуылдар да талданады. Мұндай шабуылдар бұлттық қолданба өнімділігіне әсер етіп, зиянды мақсаттар үшін ақпараттың ағып кетуіне әкелуі мүмкін.

КҚ тұрғысынан МО әдістері [22] бұлтта өте маңызды, сондықтан жақын арада әрбір бұлттық жүйе МО әдістерін қолданады.

БЕ сұранысының артуымен және жүйеге жүктеменің өсуімен, сондай-ақ трафик көлемінің өсуімен байланысты деректерді өңдеу орталықтарының (ДӨО) жұмысына белсенді мониторингтік араласу қажет болады. Бұл инфрақұрылымның үздіксіз жұмысын қамтамасыз етуге мүмкіндік береді, өйткені КҚ қауіптері мен ақауларға жедел әрекет ету жүйенің тұрақтылығы мен қауіпсіздігіне ықпал етеді. Компоненттердің күйін бақылауды және бұлттық инфрақұрылымды басқаруды қоса алғанда, мониторинг көрсетілетін қызметтердің жоғары деңгейін қамтамасыз етуде, ресурстарды бөлуді оңтайландыруда және сенімділік пен КҚ қамтамасыз етуде шешуші рөл атқарады. Бұл клиенттер үшін де, бұлтты провайдерлер үшін де бірдей маңызды. Бұлтты орта мониторингісі бірнеше ішкі типтерді қамтиды, олардың әрқайсысы өз функцияларын орындайды [23]. Атап айтқанда, КҚ мониторингісі - ықтимал қауіпті алгоритмдерді анықтау және бұлттық жүйелердің қауіпсіздігін бұзудың алдын алу.

[21, 22] жұмыстарында БЕ КҚ қамтамасыз ету контекстінде бұлтты инфрақұрылым даналары қарастырылады. Даналар - бұлтты провайдер әртүрлі тапсырмалар мен

қосымшаларды орындау үшін ұсынатын виртуалды немесе физикалық есептеу ресурстары. Бұл ресурстарға ВМ, контейнерлер, серверлер, дерекқорлар (ДҚ) және клиенттің қажеттіліктеріне сәйкес масштабтауға және конфигурациялауға болатын басқа есептеу ресурстары кіруі мүмкін. [22] авторларының пікірінше, бұлтты инфрақұрылымның даналары (ВМ немесе контейнер) бұлтты қызметтердің КҚ қамтамасыз етуде маңызды рөл атқарады.

Біріншіден, провайдерлер бұлтты инфрақұрылым даналарын құру және басқару үшін виртуализацияны жиі пайдаланады. Бұл әртүрлі клиенттер арасында ресурстарды оқшаулау мен сегменттеуді қамтамасыз етеді, бұл деректер мен қолданбаларға РҚЖ алдын алуға көмектеседі. Екіншіден, бұлтты инфрақұрылым даналары аномалияларды, ықтимал қауіптерді және рұқсат етілмеген әрекеттерді анықтау үшін пайдаланылуы мүмкін. Бұл бұлттық қызмет операторларына ықтимал қауіпсіздік оқиғаларына жедел жауап беруге және олардың алдын алуға мүмкіндік береді. Үшіншіден, БИҚ даналарын пайдалану сонымен қатар әртүрлі пайдаланушылар мен қолданбалар үшін қол жеткізу құқықтары мен КҚ саясатын реттеуге мүмкіндік береді. Бұл деректер мен ресурстарға қол жеткізуді бақылауды қамтамасыз етеді және РҚЖ алдын алуға көмектеседі. Төртіншіден, даналар DDoS шабуылдарына қарсы арнайы қорғау құралдарын қолдана отырып орнатуға болады, бұл тіпті жаппай желілік шабуылдар кезінде де қызметтердің үздіксіздігін қамтамасыз етуге көмектеседі.

Нәтижелер және талқылау.

Алдыңғы зерттеулердің талдауы көрсеткендей, деректер мен қосымшалардың бұлтты қызметтерге көбірек көшуіне байланысты КҚ бірқатар жаңа және ерекше проблемаларға тап болады. 1-кестеде бұлттық қызметтерді пайдалану кезінде пайда болған негізгі қауіптеріне жүйелі шолу келтірілген.

1 кесте - Бұлтты қызметтерді пайдалану кезінде негізгі қауіптеріне жүйелі шолу (авторлар осы зерттеуде келтірілген әдеби дереккөздерді талдау нәтижелері бойынша құрастырған)

БҚ КҚ үшін қауіп	Қауіпті жою бойынша басым шаралар
Бұлтты қызметтердегі есептік жазбаларды, құқықтарды, қол жетімділікті және парольдерді жеткіліксіз бақылау	Пайдаланушылар мен қосымшаларды дискретті оқшаулау. Қол жеткізу құқықтарын басқару үшін тиімді құралдар. Көп факторлы аутентификация (MFA). Рөлге негізделген қол жетімділікті басқару (RBAC). Күдікті әрекеттер мен РҚЖ анықтау немесе нақты уақыт режимінде басып кіру әрекетін анықтау үшін қол жетімділік аудиті және мониторинг.
Жеткіліксіз қорғалған интерфейстер мен API	Интерфейстер мен API қауіпсіздігін жүйелі түрде тексеру және бағалау оларды жүзеге асырудағы ықтимал осалдықтар мен кемшіліктерді анықтауға көмектеседі. OAuth, OpenID Connect, SSL/TLS сияқты қауіпсіздік стандарттарын пайдалану, сондай-ақ RESTful API принциптеріне сәйкес келу бұлттық қызметтердің интерфейстері мен API жұмыс істеу кезінде қорғауды қамтамасыз етуге көмектеседі. API қол жеткізу үшін қатаң авторизация жүйесін енгізу БС-ге РҚЖ алдын алуға және деректерді ағып кетуден қорғауға көмектеседі.

Қате конфигурация және БҚ өзгерістерді басқарудың жеткіліксіздігі	БҚ конфигурациясын баптау және басқару үшін автоматтандыру құралдарын пайдалану адам қателіктерінің алдын алуға және КҚ параметрлерін стандарттауды қамтамасыз етуге көмектеседі. БҚ конфигурациясының тұрақты аудиттерін жүргізу ықтимал осалдықтар мен конфигурация қателерін анықтауға және түзетуге көмектеседі. Өзгерістер мониторингі жүйелерін енгізу БҚ енгізілетін барлық өзгерістерді бақылауға және талдауға мүмкіндік береді, бұл рұқсат етілмеген әрекеттерді жедел анықтауға ықпал етеді және БҚ КҚ қатерлерінің алдын алады. Конфигурация ережелері мен өзгерістерді басқару процедураларын қоса алғанда, қатаң КҚ саясаттарын әзірлеу және енгізу мисконфигурация және рұқсат етілмеген өзгерістер қаупін азайтуға көмектеседі.
Бұлттық жүйе архитектурасына қатысты қауіпсіздік мәселелері	БҚ контекстінде бизнес мақсаттарын, тәуекелдерді, КҚ қауіптерін және заңнамаға сәйкестігін, сондай-ақ олардың инфрақұрылымының ерекшеліктерін қарастыру кезінде бұлтты қоймалардағы өзгерістердің жоғары динамикасын және шектеулі орталықтандырылған бақылауды ескеруі керек. БҚ инфрақұрылымдық стратегиясын дамытуға және бейімдеуге назар аудару қажет. Шешімдерді бейімдеу кезінде вендор ұсынатын КҚ бағалаудың негізгі тәжірибелерін ескеру қажет.
БҚ үшін қосымшаларды әзірлеуге байланысты қауіптер мен тәуекелдер	БҚ қосымшаларын қауіпсіз әзірлеу бойынша әзірлеушілерді оқыту мен сертификаттауды қамтамасыз ету КҚ туралы хабардарлықты арттыруға және кодтағы қателер қаупін азайтуға көмектеседі. БҚ қосымшаларын әзірлеу кезінде қауіпсіздік механизмдері орнатылған және осалдығы тексерілген дәлелденген фреймворктар мен кітапханаларды пайдалану керек. Статикалық және динамикалық код талдауын жүргізу құру сатысында қолданбалардағы ықтимал осалдықтар мен қателерді анықтауға көмектеседі. Артықшылықтарды азайту және ресурстарға қол жеткізуді шектеу сияқты әдепкі қорғау принциптерін ескере отырып, қолданбаларды орнату шабуыл бетін азайтуға және жүйенің бұзылу қаупін азайтуға көмектеседі.
Сыртқы компания-лар ұсынатын БҚ жұмыс істеу кезінде туындайтын қауіптер мен осалдықтар	БҚ қолданар алдында жеткізушінің қауіпсіздігіне, оның беделіне, қауіпсіздік стандарттарына, сертификаттауға және сенімділік рейтингтеріне мұқият талдау жүргізу қажет. SLA (Service Level Agreement) жасау маңызды, онда жеткізушінің қауіпсіздік міндеттемелері, соның ішінде инциденттерге жауап беру процедуралары, деректердің сақтық көшірмесі және аудитке қол жеткізу нақты анықталуы керек.

	КҚ тұрақты мониторингі мен аудитін жүзеге асыру БҚ қауіпсіздігіндегі ықтимал осалдықтар мен кемшіліктерді анықтауға, сондай-ақ олардың қауіпсіздік стандарттарына сәйкестігін бақылауға мүмкіндік береді. Инциденттерге ден қою жоспарын әзірлеу және үнемі жаңарту БҚ КҚ ықтимал қауіптеріне жедел және тиімді жауап беруге мүмкіндік береді.
БҚ жүйелік осалдықтарға байланысты қауіптер	Белгілі осалдықтарды түзету үшін бұлттық инфрақұрылымның барлық компоненттерін, соның ішінде операциялық жүйелерді, қолданбаларды және қызметтерді үнемі жаңартып, патчтау қажет. Бұлттық инфрақұрылымдағы осалдықтарды жүйелі түрде сканерлеу және бақылау КҚ ықтимал қауіптерін жедел анықтауға және жоюға көмектеседі. БҚ жүйелік ресурстар мен деректерге қол жетімділік пен артықшылықтарды шектеу осалдықтарды пайдалану қаупін азайтуға көмектеседі.
Бұлтты қоймадан ақпараттың байқаусызда ағып кетуіне байланысты қауіптер	ВМ, контейнерлерді (даналарды) және оларға орнатылған БЖ қоса алғанда, хостингте орналастырылған PaaS дерекқорларына (ДҚ), қоймаларға және ДҚ тексеру жүргізу қажет. Трафикті сырттан көрінетін кез келген түбірлік немесе желілік қызметтерді уақтылы анықтау үшін бұлттық ортаға толығымен біріктірілген іздеу машиналарын таңдау керек. Бұл шараларға жүктеме теңестіргіштері, контентті жеткізу желілері, желілік пиринг (network peering) және бұлтты брандмауэрлер кіреді. Іздеу машинасы кластерлік IP, Kubernetes қызметтері және қол жеткізу ережелері сияқты көптеген желілік компоненттерді қарастыруы керек.
Серверсіз және контейнерлік шешімдерді дұрыс конфигурацияла-мауға және қолдануға байланысты қауіптер	Ansible, Terraform немесе Kubernetes сияқты конфигурация мен деплойментті автоматтандыру құралдарын пайдалану контейнерлер мен серверсіз қолданбаларды орнату және орналастыру кезінде адам қателіктерінің алдын алуға көмектеседі. Конфигурацияны бақылау және аудит жүйелерін енгізу нақты уақыттағы мисконфигурацияларды уақтылы анықтауға және түзетуге, сондай-ақ БҚ КҚ-дегі ықтимал осалдықтарды анықтау үшін конфигурациядағы өзгерістерді бақылауға мүмкіндік береді. Least privilege принциптерін қолдану да тиімді болуы мүмкін, өйткені «ең аз артықшылықтар» қағидаты бойынша контейнерлер мен серверсіз функцияларға қол жеткізу құқықтары мен артықшылықтарын теңшеу осалдықтарды пайдалану қаупін азайтуға көмектеседі.
Ұйымдасқан қылмыстық топтардың және/немесе хакерлік топтардың әрекеттеріне байланысты қауіптер	Желіні қорғау құралдарын, firewall, кіруді анықтау жүйелерін (IDS) және кіруді болдырмау жүйелерін (IPS) орнату және қалыпты емес әрекеттерді анықтау үшін желілік трафикті үнемі бақылау.

	Екі факторлы аутентификация механизмдерін, рөлдер мен артықшылықтарға қол жеткізуді шектеуді және парольдерді үнемі жаңартуды қоса алғанда, көп деңгейлі аутентификацияны және бұлттық ресурстарға қол жеткізуді қатаң бақылауды енгізу. Деректерді шифрлауды тыныштықта және клиенттер мен бұлтты қызметтер арасында тасымалдау кезінде қолдану құпия ақпаратты РҚЖ қорғауға көмектеседі. Нақты уақыттағы КҚ ықтимал қауіптері мен инциденттерін анықтау және оларға ден қою үшін КҚ тұрақты аудиттерін және оқиғалардың мониторингін жүргізу. Деректердің сақтық көшірмесін үнемі жасау және оқиғалардан кейін қалпына келтіру жоспарларын жасау КҚ шабуылы немесе оқиғасы кезінде деректердің жоғалуын азайтуға көмектеседі.
Бұлтты сақтау деректерін эксфиль-трациялауға байланысты қауіптер	Тек қажетті пайдаланушылар мен топтарға деректерге қол жеткізу қажет болған кезде «қажеттілік» (least privilege) принципіне сәйкес бұлттық қоймаларға қатаң қол жеткізу құқықтарын орнату. Белсенділікті бақылау және қауіптерді анықтау жүйелерін енгізу бұлтқа негізделген деректер қоймаларындағы әдеттен тыс әрекеттерді анықтауға мүмкіндік береді, мысалы, үлкен көлемдегі деректерге қол жеткізу немесе жүктеу әрекеттері. Бұлтты қоймалардан құпия ақпаратты рұқсатсыз экспорттау немесе жүктеу әрекеттерін автоматты түрде анықтайтын және бұғаттай алатын деректердің бұзылуын болдырмау жүйелерін (DLP) енгізу. Бұлтты қоймалардағы деректермен қауіпсіз жұмыс істеу ережелері бойынша, сондай-ақ әлеуметтік инженерия мен фишингтік шабуылдарды тану және алдын алу бойынша қызметкерлерге оқыту және тренингтер өткізу.

БЕ және БҚ киберқауіпсіздік мәселелеріне қатысты алдыңғы зерттеулерді шолу және талдау нәтижесінде келесі қорытындылар жасауға болады:

Бұлтты есептеу және бұлтты қызметтер бизнес-процестердің тиімділігін, икемділігін және ауқымдылығын қамтамасыз етуде маңызды рөл атқарады. Алайда, бұлтты ресурстарды пайдалану қауіпсіздікке қауіп пен тәуекелдерді төндіреді. Компаниялар КҚ саласында әртүрлі қауіптерге тап болады, соның ішінде РҚЖ, клиенттердің жеке ақпаратын ұрлау және құпиялылықты бұзу. Инфрақұрылым мен деректерді қорғау маңызды міндет болып табылады.

Бұлтты даналардың жеткіліксіз қорғалуы зиянды бағдарламалардың осалдығы мен пайдаланылуына, сондай-ақ зиянкестер тарапынан рұқсатсыз қол жеткізуге әкеп соғуы мүмкін екендігі анықталды. Сонымен қатар, БҚ дұрыс емес конфигурация және басқару осалдықтардың көзі бола алады.

КҚ саласында көп факторлы аутентификация, деректерді шифрлау, аномалияларды бақылау және анықтау, сондай-ақ қолданылатын жүйелер мен бизнес-процестердің тұрақты аудиттері сияқты заманауи әдістер мен технологияларды қолдану маңызды

екендігі көрсетілген. Тек осылай ғана тәуекелдерді азайтуға және бұлттық ресурстарды, соның ішінде бұлттық қызметтерді қауіпсіз пайдалануды қамтамасыз етуге болады.

Осы мақалада талданған жұмыстарда негізінен бұлтты инфрақұрылымдардың КҚ қамтамасыз етудің кешенді тәсілі мәселесіне арналған мәселелер шеңбері талқыланады. Көптеген жұмыстарда көрсетілгендей, бұлтты есептеу дәстүрлі бизнес-процестерді жүргізу модельдерін вытыстыра отырып, тез танымал бола бастады. Алайда, талданған жұмыстар ресурстарды бөлу мониторингі жүйесін іске асыру мәселелерін жеткілікті дәрежеде қамтымайды. Сондай-ақ, қаралған жұмыстар бұлтты инфрақұрылымдардың КҚ қамтамасыз етудің МО әдістерін қолдану және жүктеудің болжамды моделін құру және даналардың КҚ көрсеткіштерін жинау әдістемесі сияқты аспектісіне айтарлықтай көңіл бөлмегені анықталды. Даналар деген - бұлтты инфрақұрылымдағы виртуалды машиналар және контейнерлер деп түсініледі. Болашақ зерттеулер шеңберінде шешуді қажет ететін негізгі мәселелердің ішінде мыналарды бөліп көрсету керек:

- КҚ саясатын бұзу салдарынан даналардың қалыптан тыс мінез-құлқын сипаттайтын жаңа модельдерді әзірлеу;
- аномальды немесе күдікті әрекеттерді анықтау мақсатында бұлтты инфрақұрылым даналарының оқиғалар журналдарын (логтарын) талдау үшін мұғаліммен МО әдістерін дамыту.

Қорытынды.

Бұлтты есептеу пайдаланушылардың тікелей басқаруынсыз сұраныс бойынша деректер қоймалары мен есептеу қуаты сияқты желілік ресурстарға қол жеткізуді қамтамасыз ететіні көрсетілген. Қазіргі уақытта БЕ клиенттерге интернет арқылы бірыңғай платформа ұсынатын мемлекеттік және жеке деректер орталықтарын қамтиды.

Көптеген зерттеулер БЕ алдында тұрған клиенттер үшін киберқауіпсіздік мәселелерін, қауіптер мен осалдықтарды көрсететіні анықталды және бұл қауіптермен күресудің перспективалы әдістерінің бірі машиналық оқыту әдістерін қолдану болып табылады.

Бұлтты құрылымдардың КҚ қауіптері мен проблемаларына талдау, сондай-ақ БЕ және БҚ қауіпсіздігін қамтамасыз ету бойынша әртүрлі авторлар ұсынған шешімдерге шолу жасалды.

ӘДЕБИЕТТЕР

[1] Khilar, P.; Vijay, C.; Rakesh, S. Trust-Based Access Control in Cloud Computing Using Machine Learning. In Cloud Computing for Geospatial Big Data Analytics; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 49, pp. 55–79.

[2] Subashini, S.; Kavitha, V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. J. Netw. Comput. Appl. 2011, 35, pp. 1–11.

[3] Bhamare, D.; Salman, T.; Samaka, M.; Erbad, A.; Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur, India, 16–20 December 2016; pp. 1–5.

[4] Yuhong, L.; Yan, S.; Jungwoo, R.; Syed, R.; Athanasios, V. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J. Comput. Sci. Eng. 2015, 9, pp. 119–133.

[5] Frolov, V.V. Analysis of approaches providing security of cloud sevices. Radioelectronic and Computer Systems, (1), 2020, pp. 70-82.

[6] Sayantan, G.; Stephen, Y.; Arun-Balaji, B. Attack Detection in Cloud Infrastructures Using Artificial Neural Network with Genetic Feature Selection. In Proceedings of the IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, Athens, Greece, 12–15 August 2016; pp. 414–419.

[7] Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. Indones. J. Electr. Eng. Comput. Sci. 2019, 16, 435.

[8] Alsolami, E. Security threats and legal issues related to Cloud based solutions. Int. J. Comput. Sci. Netw. Secur. 2018, 18, pp. 156–163.

[9] Xue, M.; Yuan, C.; Wu, H.; Zhang, Y.; Liu, W. Machine Learning Security: Threats, Countermeasures, and Evaluations. IEEE Access 2020, 8, pp. 74720–74742.

[10] Deshpande, P.; Sharma, S.C.; Peddoju, S.K. Security threats in cloud computing. In Proceedings of the International Conference on Computing, Communication and Automation, Greater Noida, India, 11–14 December 2011; pp. 632–636.

[11] Varun, K.A.; Rajkumar, N.; Kumar, N.K. Survey on security threats in cloud computing. Int. J. Appl. Eng. Res. 2014, 9, pp. 10495–10500.

[12] Kazim, M.; Zhu, S.Y. A survey on top security threats in cloud computing. Int. J. Adv. Comput. Sci. Appl. 2015, 6.

[13] Barona, R.; Anita, M. A survey on data breach challenges in cloud computing security: Issues and threats. In Proceedings of the International Conference on Circuit, Power and Computing Technologies (ICCPCT), Paris, France, 17–18 September 2017; pp. 1–8.

[14] Aawadallah, N. Security Threats of Cloud Computing. Int. J. Recent Innov. Trends Comput. Commun. 2015, 3, pp. 2393–2397.

[15] Nadeem, M. Cloud Computing: Security Issues and Challenges. J. Wirel. Commun. 2016, 1, pp. 10–15.

[16] Le Duc, T.; Leiva, R.G.; Casari, P.; Östberg, P.O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, pp. 1–39.

[17] Callara, M.; Wira, P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6.

[18] Khan, M. A survey of security issues for cloud computing. J. Netw. Comput. Appl. 2016, 71, pp. 11–29.

[19] Lin, C.; Lu, H. Response to Co-resident Threats in Cloud Computing Using Machine Learning. In Proceedings of the International Conference on Advanced Information Networking and Applications, Caserta, Italy, 15–17 April 2020; Volume 926, pp. 904–913.

[20] Venkatraman, S.; Mamoun, A. Use of data visualisation for zero-day malware detection. Secur. Commun. Netw. 2018, pp. 1–13.

[21] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.

[22] Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching cybersecurity using the cloud. IEEE Transactions on Learning Technologies, 8(4), pp. 383-392.

[23] Yau, S. S., Buduru, A. B., & Nagaraja, V. (2015, June). Protecting critical cloud infrastructures with predictive capability. In 2015 IEEE 8th International Conference on Cloud Computing (pp. 1119-1124). IEEE.

Nurbol Akhatayev, senior lecturer, at Satpayev University, Almaty, Kazakhstan, n.akatayev@satbayev.university

Evgeniya Aitkhozhaeva, candidate of technical sciences, professor, Satpayev University, Almaty, Kazakhstan, y.aitkhozhayeva@satbayev.university

Zhuldyz Alimseitova, PhD, associate professor, Satpayev University, Almaty, Kazakhstan, zhuldyz_al@mail.ru

PROBLEMS OF ENSURING CYBERSECURITY OF CLOUD INFRASTRUCTURES, A REVIEW OF PREVIOUS RESEARCH

Abstract. Cloud computing is a means of accessing network resources, such as data warehouses and computing power, on demand, without direct user control. Currently, companies use both public and private data centers that provide customers with a single platform over the Internet. In addition, edge computing is actively used, which allows you to bring computing and information storage closer to end users in order to optimize cloud services. However, in the use of cloud computing, cybersecurity issues arise related to threats and vulnerabilities for customers. This publication presents an analysis of scientific publications devoted to the problems of ensuring cybersecurity of cloud computing and cloud services.

Keywords. Cloud computing, cybersecurity, threats, cyberattacks, anomalies.

Нурбол Акатаев, старший преподаватель, Satpayev University, Алматы, Казахстан, n.akatayev@satbayev.university
Евгения Айтхожаева, к.т.н., профессор, Satpayev University, Алматы, Казахстан, y.aitkhozhayeva@satbayev.university
Жулдыз Алимсеитова, PhD, ассоциированный профессор, Satpayev University, Алматы, Казахстан, zhuldyz_al@mail.ru

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ОБЛАЧНЫХ ИНФРАСТРУКТУР, ОБЗОР ПРЕДШЕСТВУЮЩИХ ИССЛЕДОВАНИЙ

Аннотация. Облачные вычисления представляют собой средства доступа к сетевым ресурсам, таким как хранилища данных и вычислительные мощности, по требованию, без прямого управления со стороны пользователей. В настоящее время компании используют как публичные, так и частные центры обработки данных, предоставляющие клиентам единую платформу через интернет. Кроме того, активно применяются периферийные вычисления (edge computing), которые позволяют приблизить вычисления и хранение информации к конечным пользователям для оптимизации облачных сервисов. Однако, в использовании облачных вычислений, возникают проблемы кибербезопасности, связанные с угрозами и уязвимостями для клиентов. В данной публикации представлен анализ научных публикаций, посвященных проблематике обеспечения кибербезопасности облачных вычислений и облачных сервисов.

Ключевые слова. Облачные вычисления, кибербезопасность, угрозы, кибератаки, аномалии.

****