ҒТАХР 14.35.07

10.51889/2959-5894.2025.92.4.014

Г.Б. Елубай[1*], Б.С. Ахметов[1], В.А. Лахно[2]

[1]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан
[2]Ұлттық биоресурстар және табиғатты пайдалану университеті, Киев қ., Украина
[*]*e-mail: g.elubaeva@abaiuniversity.edu.kz*

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТАЛАПТАРЫНА СӘЙКЕС ЖЕКЕ УНИВЕРСИТЕТТІК VDI БҰЛТЫНЫҢ МАТЕМАТИКАЛЫҚ МОДЕЛІ

Аңдатпа

Мақалада виртуалды жұмыс орындарын (VDI) қолдана отырып, жеке университеттің бұлтты есептеу түйіндерінің оңтайлы санын бағалаудың кеңейтілген математикалық моделі және университеттердің бұлтқа бағытталған оқу ортасының (ББОО) ақпараттық қауіпсіздік талаптары ұсынылған. Бұрынғы белгілі тәсілдерден айырмашылығы, әзірленген модель ресурстық жүктемені (CPU, RAM) ғана емес, сонымен қатар виртуалды машиналар мен серверлердің қауіпсіздік деңгейіне қойылатын талаптарды да ескереді. Ұсынылған модельде ББОО қауіпсіздігінің сандық параметрлері енгізілген және виртуалды машинаны орналастыру міндеті ресурстарды пайдалану тиімділігі мен ББОО қауіпсіздік талаптарын сақтау арасындағы тепе-теңдікті сақтайтын көп өлшемді оңтайландыруға дейін азаяды. Ұсынылған тәсілдің практикалық маңыздылығын растайтын университеттің АТ-инфрақұрылымының типтік параметрлерімен бұлттың жұмысын имитациялық модельдеу жүргізілді. Модель ҚР университеттерінің білім беру ортасында қорғалған бұлтты платформаларды жобалау үшін қолдануға болады.

Түйін сөздер: жеке бұлт, VDI, виртуализация, университеттің АТ инфрақұрылымы, ақпараттық қауіпсіздік, математикалық модель.

Г.Б. Елубай[1], Б.С. Ахметов[1], В.А. Лахно[2]
[1]Казахский национальный педагогический университет имени Абая, г.Алматы, Казахстан
[2] Национальный университет биоресурсов и природопользования г.Киев, Украина

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ VDI-ОБЛАКА ЧАСТНОГО УНИВЕРСИТЕТА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В статье предложена расширенная математическая модель оценки оптимального количества вычислительных узлов частного университетского облака с использованием виртуальных рабочих мест (VDI), и с учетом требований информационной безопасности облако-ориентированной учебной среды (ООУС) университетов. В отличие от ранее известных подходов, разработанная модель учитывает не только ресурсную нагрузку (CPU, RAM), но и требования к уровню защищенности виртуальных машин и серверов. В предлагаемой модели введены количественные параметры защищенности ООУС, а задача размещения ВМ сведена к многокритериальной оптимизации, балансирующей между эффективностью использования ресурсов и соблюдением требований безопасности ООУС. Проведена имитационная симуляция работы облака с типичными параметрами университетской ИТ-инфраструктуры, подтверждающая практическую значимость предложенного подхода. Модель целесообразна для проектирования защищенных облачных платформ в образовательной среде университетов РК.

Ключевые слова: частное облако, VDI, виртуализация, университетская ИТ-инфраструктура, информационная безопасность, математическая модель.

G.B. Yelubay, B.S. Akhmetov, V.A. Lakhno
[1]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan
[2] National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine

MATHEMATICAL MODEL OF A PRIVATE UNIVERSITY'S VDI CLOUD IN COMPLIANCE WITH INFORMATION SECURITY REQUIREMENTS

Abstract

The article offers an extended mathematical model for estimating the optimal number of computing nodes in a private university cloud using virtual workstations (VDI), and taking into account the information security requirements of a cloud-based learning environment (OSS) of universities. Unlike previously known approaches, the developed model takes into account not only the resource load (CPU, RAM), but also the requirements for the security level of virtual machines and servers. In the proposed model, quantitative parameters of the security of the OSS are introduced, and the task of VM deployment is reduced to a multi-criteria optimization balancing between resource efficiency and compliance with the security requirements of the OSS. A simulation simulation of the cloud operation with typical parameters of the university IT infrastructure has been carried out, confirming the practical significance of the proposed approach. The model is suitable for designing secure cloud platforms in the educational environment of universities of the Republic of Kazakhstan.

Keywords: private cloud, VDI, virtualization, university IT infrastructure, information security, mathematical model.

Кіріспе

Осы мақалада Қазақстан Республикасының университеттері мен білім беру мекемелеріне арналған бұлтқа бағытталған оқу ортасында (ББОО) виртуалды жұмыс орындарын (VDI) орналастыруға арналған жекеменшік бұлт инфрақұрылымын оңтайлы жобалаудың жаңа тәсілі ұсынылады. Ерекшелігі – есептеу ресурстарын жоспарлау кезінде тек техникалық сипаттамалар емес, сонымен қатар ақпараттық қауіпсіздік талаптары, атап айтқанда, серверлердің сенім деңгейі, қолжетімділік пен оқшаулау саясаты, сондай-ақ ішкі және сыртқы қауіптерге төзімділік секілді аспектілер ескеріледі. Ұсынылған тәсіл ББОО-ға тән жүктеменің маусымдық және динамикалық сипатын ескере отырып, виртуализацияланған инфрақұрылымды икемді масштабтауды қамтамасыз етуге және қауіпсіздікті сақтай отырып ресурстарды тиімді пайдалануға мүмкіндік береді. Университеттер мен басқа да білім беру мекемелерінде (мектептер, колледждер және т.б.) жекеменшік бұлттар негізінде виртуалды жұмыс орындары (VDI) инфрақұрылымын енгізу ортақ есептеу ресурстарын тиімді пайдалануға мүмкіндік береді. Сонымен қатар, Қазақстан (ҚР) университеттері үшін бұл тәсіл пайдаланушылардың ағымдағы қажеттіліктері мен бұлтты университеттік инфрақұрылымға жүктеме деңгейіне байланысты икемді масштабтауды жүзеге асыруға жол ашады. Мақалада ұсынылған тәсіл ҚР университеттері мен ғылыми-білім беру мекемелеріне, ақпараттық технологиялық ортасы сессия кезеңдерінде жүктеменің қарқынды өзгеруімен және бұлтты инфрақұрылымның ақпараттық қауіпсіздігіне қойылатын жоғары талаптармен сипатталатын ұйымдарға, өзекті болып табылады. Университеттің бұлтты инфрақұрылымына (немесе [1, 2] деректеріне сәйкес – бұлтқа бағытталған оқу ортасына – ББОО) түсетін жүктеменің өзгермелілігі мен пайдаланушылар талаптарының әртүрлілігін ескере отырып, бұлтты платформаның тұрақты және қауіпсіз жұмысын қамтамасыз ету үшін қажет есептеу түйіндерінің (серверлердің) санын бағалау мәселесі өзекті болып отыр. Бұған дейін ұсынылған VDI-бұлттарындағы кластер түйіндерінің санын бағалауға арналған математикалық модельдер [3, 4] әдетте, ресурстық жүктемені талдауға [5–7] негізделіп, виртуалды машиналардың ресурстарды тұтыну параметрлері берілген жағдайда физикалық серверлер санын азайту тиімділіктің негізгі өлшемі деп қарастырады. Алайда біз бұл тәсілдер бұлтқа бағытталған оқу ортасының (ББОО) принципті аспектісі – ақпараттық қауіпсіздікті (АҚ), оның ішінде физикалық түйіндерге деген сенім деңгейін, оқшаулау талаптарын, қолжетімділік саясатын және ішкі/сыртқы қатерлерге төзімділікті ескерусіз қалдырады деп санаймыз [8–11].

Зерттеу әдіснамасы

Университеттің бұлтқа бағытталған оқу ортасы (ББОО) үшін келесі шарттарды қамтамасыз ететін есептеу түйіндерінің (М) ең аз қажетті санын анықтау:

- виртуалды машиналарды (ВМ) ресурстарды (CPU, RAM және т.б.) ескере отырып дұрыс орналастыру;
- ақпараттық қауіпсіздік талаптарын (оқшаулау, түйіндерге деген сенім) қанағаттандыру;
- динамикалық жүктемеге бейімделу және жекеменшік бұлттың (ҚР университеті мысалында) масштабталуы.

Зерттеу нәтижелері

Келесі белгілерді енгізейік. Сәйкесінше университеттің ББОО серверлері үшін.

$M -$ ББОО университетінің қол жетімді физикалық серверлерінің (түйіндерінің) жалпы саны;

$R -$ ресурстар түрлерінің жалпы саны (мысалы, CPU, RAM, және т.б.);

$C_{jk} -$ j серверіндегі k ресурсының сыйымдылығы, $j \in \{1, \dots, M\}, k \in \{1, \dots, R\}$;

$S_j \in [0,1] -$ j серверінің қауіпсіздік (сенім) деңгейі. Яғни, S_j неғұрлым жоғары болса, ББОО соғұрлым қауіпсіз болады.

Және ВМ параметрлеріне де ұқсас түрде.

$N -$ Университеттің ББОО-сында (бұлтқа бағытталған оқу ортасында) орналастырылуы қажет виртуалды машиналар (ВМ) саны.;

$active(t) \subseteq \{1, \dots, N\} -$ t уақыт мезетіндегі белсенді виртуалдық машиналар жиынтығы;

$r_{jk} -$ t уақыт мезетінде ВМ үшін ең аз қажетті k типті ресурстар;

$a_j(t) -$ t уақыт мезетінде виртуалды машинаның (ВМ) нақты CPU тұтынуы;

$H_i \in [0,1] -$ t уақыт мезетінде виртуалды машина (ВМ) үшін талап етілетін қауіпсіздік деңгейі.

Сонымен қатар, біз осындай айнымалыларды қолданамыз:

$x_{ij}(t) \in \{0,1\} -$ егер ВМ i уақыттың t мезетінде j серверіне орналастырылса – мәні 1, орналастырылмаса – 0-ге тең болатын бинарлық айнымалы;

$y_j(t) \in \{0,1\} -$ t уақыт мезетінде сервер j-дің пайдаланылып-пайдаланылмайтыны, яғни бұл әдетте бинарлық айнымалымен белгіленеді:

1 - егер сервер сол уақытта нақты ВМ-дерді орналастырып, жұмыс істеп тұрса;

0 - егер сервер бос немесе өшірулі күйде болса;

$\alpha \in [0,1] -$ қауіпсіздік резервтеу деңгейі (ББОО университетінің қауіпсіздігін бағалау кезіндегі агрессивтілік коэффициенті);

$\lambda > 0 -$ ББОО қауіпсіздігінің сәйкес келмеуі үшін айыппұл коэффициенті.

Біз келесі шектеулерді қолданамыз.

Әрбір ВМ бір серверде орналастырылған, яғни.

$$\sum_{j=1}^{M} x_{ij}(t) = 1, \forall\, i \in active(t).$$

Әрбір ББОО серверіндегі ресурстар бойынша шектеу.

Әр ресурс үшін k

$$\sum_{i \in active(t)} x_{ij}(t) \cdot r_{jk} \le C_{jk}, \forall j, \forall k.$$

Онда CPU үшін,

$$\sum_{i \in active(t)} x_{ij}(t) \cdot a_j(t) \le C_j^{CPU}, \forall j.$$

Онда [3, 7] еңбектерінен айырмашылығы ретінде университеттің ББОО-сына (бұлтқа бағытталған оқу ортасына) қатысты қауіпсіздік шектеуін енгіземіз (қатаң немесе жұмсақ тәсіл).

Қатаң тәсіл

$$x_{ij}(t) = 1 \Rightarrow S_j \geq R_i(t).$$

Айыппұл салумен жұмсақ тәсіл

$$x_{ij}(t) \cdot max\big(0, R_i(t) - S_j\big) \geq 0.$$

Сонымен қатар, университеттің ББОО-сында түйіндердің ең төменгі рұқсат етілетін қорғалу деңгейін белгілеуге болады.:

$$S_j \geq S_{min}.$$

Онда мақсатты функцияның екі нұсқасын қарастырамыз.

1-нұсқа – екі критерийлі есеп (университеттің ББОО-сындағы ақпараттық қауіпсіздік пен қаржы үнемділігін қатар ескеру).

$$min\{\sum_{j=1}^{M} y_i(t) + \lambda \cdot \sum_{i,j} x_{ij}(t) \cdot max\big(0, R_i(t) - S_j\big)\},$$

мұндағы бірінші қосылғыш – университеттің ББОО-сында пайдаланылған серверлер саны (ресурстық тиімділік), ал екінші қосылғыш – қауіпсіздік талаптарының бұзылуы үшін салынатын айыппұлдар сомасы.

2 нұсқа-өлшенген критерийлік түрлендіру

$$min\left\{\beta \cdot \sum_{j} y_i(t) + (1-\beta) \cdot \sum_{i,j} x_{ij}(t) \cdot max\big(0, R_i(t) - S_j\big)\right\}$$

мұндағы β-қауіпсіздікпен салыстырғанда тиімділіктің маңыздылық дәрежесі.

Содан кейін біз M(t) төменгі бағасын есептейміз.

[3, 7] еңбектеріндегі сияқты, университеттің ББОО-сындағы ақпараттық қауіпсіздік пен оның масштабталуын қамтамасыз ететін жаңа ішкі жиындарды ескере отырып, Мартелло-Тосс бағалау әдісін кеңейтілген түрде қолданамыз:

$\alpha_1(t) = \{i \in active(t) | \alpha_i(t) > C_{CPU} - \alpha\}$ – «үлкен» ВМ;

$$\alpha_2(t) = \{i | C_{CPU} - \alpha \geq \alpha_i(t) > 0{,}5 \cdot C_{CPU}\};$$

$$\alpha_3(t) = \{i | 0{,}5 \cdot C_{CPU} \geq \alpha_i(t) > \alpha\}.$$

Содан кейін төменгі шекараны бағалау үшін біз осындай тәуелділікті қолданамыз:

$$M_1(\alpha, t) = |\alpha_1(t) + \alpha_2(t)| + \\ + max\left(0, \frac{\sum_{i \in \alpha_3(t)} \alpha_i(t) - \big(C_k \cdot |\alpha_2(t)| - \sum_{i \in \alpha_2(t)} \alpha_i(t)\big)}{C_k}\right).$$

немесе

$$M_2(\alpha, t) = |\alpha_1(t) + \alpha_2(t)| + \\ + max\left(0, \alpha_3(t) - \sum_{i \in \alpha_2(t)} \left\lfloor \frac{C_k - \alpha_i(t)}{\alpha} \right\rfloor\right).$$

Онда соңғы бағалау

$$M(t) = \max_{\alpha \in [0, 0.5]} \big(M_1(\alpha, t), M_2(\alpha, t)\big).$$

Сондай-ақ, университеттің ББОО динамикалық масштабтауын ескереміз. Тиісінше, ең жоғары жүктемелер кезінде бағалау мүмкіндігі келесідей жазылады:

$$t^* = \arg\max_t \left(\sum_{i,j} x_{ij}(t) \cdot \alpha_i(t) \right),$$
$$M_{peak} = M(t^*).$$

Дискуссия

Бұл жұмыста ЖРН AP19678846 «Цифрлық трансформация жағдайында жоғары оқу орындарының инфрақұрылымын дамыту негізінде оқу процесін ұйымдастырудың гибридті және қашықтық нысандарының тиімділігін арттыру» гранты аясында жүргізілген зерттеу шеңберінде университеттік ортада виртуалды жұмыс орындары инфрақұрылымын жүзеге асыруға бағытталған жекеменшік бұлтты виртуализация кластері үшін есептеу түйіндерінің оңтайлы санын бағалаудың математикалық моделі әзірленіп, формализацияланды. Бар [3, 7] еңбектерде келтірілген бұрынғы тәсілдерден ерекшелігі – ұсынылған модельдің жаңалығы мынада: алғаш рет университеттің бұлтқа бағытталған оқу ортасындағы (ББОО) ақпараттық қауіпсіздік параметрлері енгізілді. Сонымен қатар, виртуалды машиналарды орналастыруды модельдеу барысында есептеу түйіндерінің қорғалу деңгейі мен виртуалды машиналар тарапынан қойылатын қауіпсіздік талаптарының сандық сипаттамалары енгізілді. Бұл өз кезегінде нақты университеттің ББОО инфрақұрылымын жобалау кезінде қауіпсіздіктің әкімшілік және техникалық аспектілерін ескеруге мүмкіндік береді. Сондай-ақ жүктеме мен қорғалу деңгейінің уақыт бойынша динамикасы ескерілді. Яғни мақалада баяндалған модель ББОО-да виртуалды машиналар тарапынан ресурстарға қойылатын сұраныстың уақыт өте өзгеріп отыратын құрылымын, сондай-ақ олардың ақпараттық қауіпсіздікке қойылатын талаптарының динамикалық өзгеру мүмкіндігін есепке алады. Кластер түйіндерінің қажетті санына арналған төменгі және жоғарғы шектер кеңейтіліп, Мартелло - Тосс әдісін бейімдеуге негізделген жаңа бағалау формулалары ұсынылды. Бұл формулалар виртуалды машиналардың ресурстық қажеттіліктері мен физикалық түйіндердің қорғалу деңгейіне қойылатын шектеулерді бір мезгілде ескеруге мүмкіндік береді. Сондай-ақ университеттің ББОО-сындағы ВМ-ді орналастырудың көпкритерийлі оңтайландыру есебі одан әрі дамытылып, сапа функциясы ұсынылды. Ол бір мезетте пайдаланылатын физикалық түйіндер санын азайту критерийін және қорғалу деңгейінің сәйкес келмеуі үшін айыппұл критерийін қамтиды, бұл өз кезегінде ББОО инфрақұрылымының тиімділігі мен қауіпсіздігі арасында икемді тепе-теңдік орнатуға мүмкіндік береді.

Жалпы алғанда, ұсынылған модель ақпараттық қауіпсіздікке (АҚ) жоғары талаптар қойылатын жағдайларда жекеменшік университеттік бұлтты масштабтау міндеттерін шешуде неғұрлым дәл әрі өзекті нәтижелер алуға мүмкіндік береді және ҚР университеттерінің қорғалған бұлттық ортасындағы ресурстарды басқарудың зияткерлік жүйелерін синтездеу үшін базалық негіз ретінде қолайлы болып табылады.

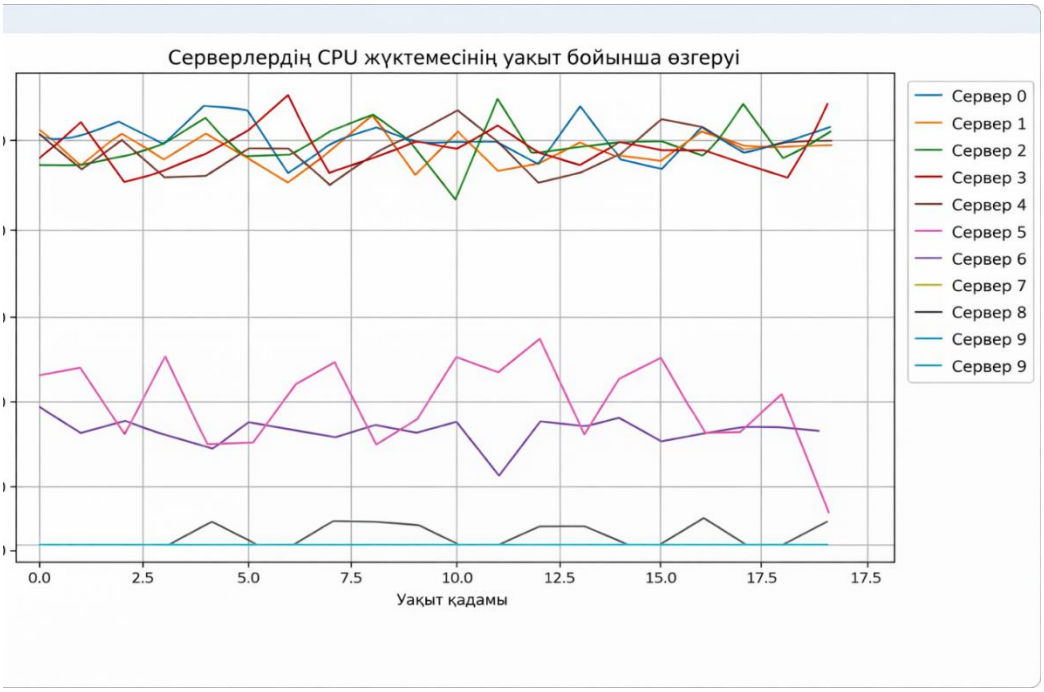
Әзірленген математикалық модельді апробациялау үшін ресурстық және ақпараттық қауіпсіздік (АҚ) талаптарын ескере отырып, университеттің жекеменшік бұлтында виртуалды машиналарды (ВМ) орналастыру бойынша имитациялық модельдеу жүргізілді. Модель Python ортасында жүзеге асырылып, серверлер саны шектеулі жағдайдағы ББОО (бұлтқа бағытталған оқу ортасы) шеңберінде жүктемені тарату мен ақпараттық қауіпсіздік талаптарының орындалуын талдауға мүмкіндік берді. Нәтижелер 1-суретте көрсетілген.

Симуляция барысында әрқайсысы 100 шартты бірлік көлеміндегі есептеу қуатына және нақты қорғалу деңгейіне ие 10 физикалық серверден тұратын бұлттық инфрақұрылым қарастырылды $S_j \in [0.6,1.0]$. Виртуалды машиналардың саны – 50 деп алынды (N = 50), олардың әрқайсысы CPU ресурстарының базалық тұтынуы бойынша әртүрлі (5-тен 20 шартты бірлікке дейінгі диапазонда) және орналастыру платформасына қойылатын жеке қауіпсіздік

деңгейі талаптарына ие. Уақыт бойынша T = 20 дискретті қадам қабылданды (ООУС серверлерінің жүктеме динамикасын эмуляциялау үшін).

Әрбір уақыттық қадамда барлық виртуалды машиналарды (ВМ) серверлерге орналастыру әрекеті орындалады. Орналастырудың сәтті болуы келесі шарттардың бір уақытта орындалуына байланысты:

- серверде қолжетімді CPU ресурстарының жеткіліктілігі;
- сервердің қорғалу деңгейінің ВМ-нің қауіпсіздік талаптарына сәйкестігі. ВМ $S_j \geq R_i$.



Сурет 1. Уақыт бойынша ББОО университетінің серверлерін жүктеуді модельдеуге арналған есептеу экспериментінің графигі

Симуляция нәтижелері 1-суретте әрбір сервердің уақыт бойынша CPU жүктемесі түрінде график түрінде көрсетілген. Талдау орташа белсенділік кезеңдерінде жүктеменің серверлер арасында біркелкі бөлінетінін көрсетті. Ал жүктеменің мерзімді шарықтау сәттері университеттің бұлтқа бағытталған оқу ортасы (ББОО) инфрақұрылымының статикалық конфигурациясы жағдайында барлық талаптарды қанағаттандырудың күрделілігін айғақтайды. Серверлердің жүктелу дәрежесіндегі айқын айырмашылықтар олардың қорғалу деңгейі бойынша жүргізілген сүзгілеумен түсіндіріледі.

Симуляция барысында ресурстар тапшылығы мен серверлерге деген сенім деңгейінің жеткіліксіздігі жағдайында жүйенің бірқатар ВМ-ді орналастыра алмағаны тіркелді. Атап айтқанда, шамамен 40 жағдайда ВМ-нің орналастырылмауы орын алды, бұл көбінесе қауіпсіздікке жоғары талап қоятын ВМ-дердің бүкіл симуляция бойы орналастырыла алмаған уақыттық қадамдарында байқалды.

Жалпы алғанда, жүргізілген симуляция жекеменшік университеттік бұлт архитектурасын жобалау кезінде ақпараттық қауіпсіздік талаптарын ескерудің қажеттілігін дәлелдейді. Мақалада ұсынылған модель көрсеткендей, қорғалу деңгейіне қойылатын талаптарды ескермеу есептеу түйіндерінің қажетті санын бағалау кезінде ресурстардың жартылай қолжетімсіз болу қаупіне әкелуі мүмкін, тіпті CPU ресурстары формалды түрде жеткілікті болған жағдайда да.

Қорытынды

ЖРН AP19678846 «Цифрлық трансформация жағдайында жоғары оқу орындарының инфрақұрылымын дамыту негізінде оқу процесін ұйымдастырудың гибридті және қашықтық нысандарының тиімділігін арттыру» аясында университеттің бұлтқа бағытталған оқу ортасының (ББОО) техникалық шектеулері мен ақпараттық қауіпсіздік (АҚ) талаптарын ескере отырып, жекеменшік университеттік виртуализация бұлтындағы есептеу түйіндерінің оңтайлы санын бағалауға арналған математикалық модель әзірленді.

Қолданыстағы тәсілдерден айырмашылығы, ұсынылған модель ББОО серверлерінің сенімділік деңгейін және виртуалды машиналардың қауіпсіздік талаптарын ескеруге мүмкіндік береді. Бұл ақпараттық қауіпсіздік (АҚ) тәуекелдерін формализациялап, оларды мақсатты функция құрамына қосуға жол ашады. Соның нәтижесінде ресурстық тиімділік пен университеттік ББОО қауіпсіздігі арасында тепе-теңдік орнатуға бағытталған ВМ-дерді орналастырудың көпкритерийлі оңтайландыру есебін құру мүмкін болды.

Python бағдарламалау ортасында жүргізілген симуляция АҚ факторларын елемеу кейбір ВМ-дерді орналастыра алмауға әкелетінін көрсетті, тіпті кластердің жалпы есептеу қуаты жеткілікті болып көрінген жағдайда да. Бұл нәтижелер университеттің бұлттық инфрақұрылымын жоспарлау және масштабтау модельдеріне ақпараттық қауіпсіздік саясатын кіріктірудің өзектілігін растайды.

Біз әзірленген модель ақпараттық қауіпсіздік талаптарын ескере отырып, жүктемені бейімделген түрде теңгеруге бағытталған білім беру саласындағы интеллектуалды бұлтты басқару жүйелерін жобалауға негіз бола алады деп есептейміз.

Алғыс

Бұл зерттеу мақаласы Қазақстан Республикасы Білім және ғылым министрлігінің Ғылым комитеті қаржыландыратын «Цифрлық трансформация жағдайында жоғары оқу орындарының инфрақұрылымын дамыту негізінде оқу процесін ұйымдастырудың гибридті және қашықтық нысандарының тиімділігін арттыру» (ИРН AP19678846) жобасы аясында орындалды.

Пайдаланылған дереккөздер тізімі

[1] Литвинова, С. Г. (2014). Понятия и основные характеристики облако ориентированной учебной среды школы. Информационные технологии и средства обучения, 40(2), 26-41.

[2] Шевченко, В. Г., & Лавріненко, В. М. (2017). Формування професійної компетентності у майбутніх фахівців екологів під час лабораторних занять з екологічних біотехнологій. Наукові записки. Серія: Проблеми методики фізико-математичної і технологічної освіти, 4(11).

[3] Аверьянихин, А.Е., Котельницкий, А. В., & Муравьев, К. А. (2016). Методика расчета оптимального числа узлов кластера виртуализации частного облака виртуальных рабочих столов по критерию эффективности. Международный научно-исследовательский журнал, (5-3 (47)), 6-13. DOI: https://doi.org/10.18454/IRJ.2016.47.187

[4] Ворожцов А.С., Тутова Н.В., Тутов А.В. Методика оптимального распределения виртуальных серверов в центрах обработки данных // T-Comm: Телекоммуникации и транспорт. – 2015. – Том 9. – №7. – С. 5-10.

[5] Tutov A.V. Models and methods of resources allocation of infocommunication system in cloud data centers. H&ES Research. 2018. Vol. 10. No. 6. Pp. 100–00. doi: https://doi.org/10.24411/2409-5419-2018-10192

[6] Воробьев, А. А., & Данг, С. Б. (2016). Формализация задач оптимизации размещения виртуальных машин и распределения сетевых ресурсов в облачной вычислительной системе. Системы управления и информационные технологии, (3), 28-32.

[7] Bichler M., Speitkamp B. A Mathematical Programming Approach for Server Consolidation Problems in VirtualizedData Centers - Ieee transactions on services computing. 2010 VOL.3 p.4. DOI Bookmark: 10.1109/TSC.2010.25

[8] Ахметов, Б., & Лахно, В. (2022). Защита информации и кибербезопасность цифровой образовательной среды университета. Вестник КазАТК, 120(1), 134-141. https://doi.org/10.52167/1609-1817-2022-120-1

[9] Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589. DOI: https://doi.org/10.3390/app12052589

[10] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. DOI: https://doi.org/10.3390/fi13020039

[11] Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in universities: an evaluation model. SN Computer Science, 4(5), 569. DOI: https://doi.org/10.1007/s42979-023-01984-x

References

[1] Litvinova, S. G. (2014). Ponyatiya i osnovnye harakteristiki oblako orientirovannoj uchebnoj sredy shkoly [Concepts and main characteristics of a cloud-based learning environment for schools]. Informacionnye tekhnologii i sredstva obucheniya, 40(2), 26-41. (In Russian)

[2] Shevchenko, V. G., & Lavrinenko, V. M. (2017). Formuvannya profesijnoï kompetentnosti u majbutnih fahivciv ekologiv pid chas laboratornih zanyat' z ekologichnih biotekhnologij [Formation of professional competence among future environmental specialists during laboratory classes on environmental Biotechnologies]. Naukovi zapiski. Seriya: Problemi metodiki fiziko-matematichnoï i tekhnologichnoï osviti, 4(11). (In Ukraine)

[3] Aver'yanihin, A. E., Kotel'nickij, A. V., & Murav'ev, K. A. (2016). Metodika rascheta optimal'nogo chisla uzlov klastera virtualizacii chastnogo oblaka virtual'nyh rabochih stolov po kriteriyu effektivnosti [Methodology for calculating the optimal number of nodes in a private cloud virtualization cluster of virtual desktops based on the efficiency criterion]. Mezhdunarodnyj nauchno-issledovatel'skij zhurnal, (5-3 (47)), 6-13. DOI: https://doi.org/10.18454/IRJ.2016.47.187 (In Russian)

[4] Vorozhcov A.S., Tutova N.V., Tutov A.V. (2015) Metodika optimal'nogo raspredeleniya virtual'nyh serverov v centrah obrabotki dannyh [The methodology of optimal distribution of virtual servers in data centers]. T-Comm: Telekommunikacii i transport. Tom 9. №7. 5-10. (In Russian)

[5] Tutov A.V. Models and methods of resources allocation of infocommunication system in cloud data centers. H&ES Research. 2018. Vol. 10. No. 6. Pp. 100–00. doi: https://doi.org/10.24411/2409-5419-2018-10192

[6] Vorob'ev, A. A., & Dang, S. B. (2016). Formalizaciya zadach optimizacii razmeshcheniya virtual'nyh mashin i raspredeleniya setevyh resursov v oblachnoj vychislitel'noj sisteme [Formalization of optimization tasks for virtual machine allocation and network resource allocation in a cloud computing system]. Sistemy upravleniya i informacionnye tekhnologii, (3), 28-32. (In Russian)

[7] Bichler M., Speitkamp B. A Mathematical Programming Approach for Server Consolidation Problems in VirtualizedData Centers - Ieee transactions on services computing. 2010 VOL.3 p.4. DOI Bookmark: 10.1109/TSC.2010.25

[8] Ahmetov, B., & Lahno, V. (2022). Zashchita informacii i kiberbezopasnost' cifrovoj obrazovatel'noj sredy universiteta [Information protection and cybersecurity of the university's digital educational environment]. Vestnik KazATK, 120(1), 134-141. https://doi.org/10.52167/1609-1817-2022-120-1 (In Russian)

[9] Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589. DOI:1 https://doi.org/10.3390/app12052589

[10] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39. DOI: https://doi.org/10.3390/fi13020039

[11] Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in universities: an evaluation model. SN Computer Science, 4(5), 569. DOI: https://doi.org/10.1007/s42979-023-01984-x