https://doi.org/10.31891/2219-9365-2022-72-4-10
УДК 371.64:378.14:004

Ігор МУЛЯР
Хмельницький національний університет
https://orcid.org/0000-0002-6659-605X
muliariv@khmnu.edu.ua
Віталій ГАВРОНСЬКИЙ
Хмельницький політехнічний фаховий коледж
Національного університету»Львівська політехніка»
https://orcid.org/0000-0002-1529-1272
gavronskiy@gmail.com
Іван ГУРМАН
Хмельницький національний університет
https://orcid.org/0000-0002-2282-3484
hurmani@khmnu.edu.ua
Андрій ВІХТЮК
Хмельницький національний університет
e-mail: andrii.pain@gmail.com
Віталій ПІСТОЛЮК
Хмельницький національний університет
e-mail: Logic11@i.ua

ВИКОРИСТАННЯ СУЧАСНИХ ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ ДЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ В ХМАРНОМУ СЕРЕДОВИЩІ

В роботі вирішено актуальну науково-технічну задачув із розробкаи методу розмежування доступу до сервісів хмарного середовища, за рахунок динамічно сформованих правил фільтрації для віртуальних брандмауерів. Запропонована в роботі модель враховує динамічний характер розподілу виділених ресурсів і характеристики протоколів мережевої взаємодії. На вхід моделі надходить потік мережних пакетів, що в режимі реального часу надходять на фаєрвол системи захисту в хмарному середовищі. Модель здійснює розділення пакети на віртуальні з'єднання, та визначає підмножини правил фільтрації для всіх інформаційних з'єднань, що дозволяють фільтрувати мережеву взаємодію для дотримання політики доступу. Взаємодія віртуальних машин в рамках одного гіпервізора здійснюється без використання фізичних ліній зв'язку і забезпечується програмним методом, наприклад за рахунок використання смарт-контрактів.

Ключові слова: моделі, алгоритми, хмарне середовище, блокчейн.

Ihor MULIAR, Vitaliy GAVRONSKIY, Ivan HURMAN,
Andrii VIKHTIUK, Vitalii PISTOLIUK
Khmelnytskyi National University

USE OF MODERN DECENTRALIZED TECHNOLOGIES FOR DISTRIBUTION OF ACCESS IN THE CLOUD ENVIRONMENT

The work solves the actual scientific and technical problem of developing a method of demarcating access to cloud services using dynamically generated filtering rules for virtual firewalls. The model proposed in the work takes into account the dynamic nature of the allocation of allocated resources and the characteristics of network interaction protocols. The input of the model receives a stream of network packets that are sent to the firewall of the protection system in the cloud environment in real time. The model divides packets into virtual connections, and defines subsets of filtering rules for all information connections that allow filtering network interaction to comply with access policie.

The integration of access control functions into the components of the cloud environment reduces its performance, provided that the firewalls that control information interaction use the hardware resources of the regular hypervisor. The virtual connection classification algorithm proposed in the work uses the existing technologies of parallel computing and the structure of the TCP/IP stack, and is implemented using the Netgraph network subsystem. This makes it possible to increase the performance of firewalls and more efficiently use the computing power of existing hardware platforms. This reduces the cost of access delimitation tools in the cloud environment. The developed algorithms and method expand the possibilities of using the technology of inter-network shielding. The interaction of virtual machines within the framework of one hypervisor is carried out without the use of physical communication lines and is ensured by a software method, for example through the use of smart contracts.

Keywords: models, algorithms, cloud environment, blockchain

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Сьогодні до хмарних технологій та реалізації на їх основі середовища хмарних обчислень проявляється великий інтерес, а технологічно розвинені корпорації тадержави їх уже реалізували та широко

застосовують. В Україні Доктрина інформаційної безпеки визначає поняття інформаційної сфери як сукупність інформаційної інфраструктури, інформації, суб'єктів, які збирають, формують, поширюють та використовують інформацію, а також систему регулювання суспільних відносин, що при цьому виникають [1].

Інформаційна безпека в широкому розумінні - це такий стан об'єкта захисту, який виключає можливість пошкодження властивостей об'єкта внаслідок його взаємодії з інформаційною сферою.

Актуальною завдачою розмежування доступу є формалізація вимог щодо обмеження доступу до інформаційних сервісів у середовищі хмарних обчислень, які можуть бути представлені за допомогою динамічно сформованого набору правил фільтрації, які забезпечують відповідність вимогам політиці безпеки.

Метою дослідження є вдосконалення методу формування правил фільтрації для розмежування доступу в хмарному середовищі. Ряд публікацій присвячений аналізу існуючих загроз, побудові моделей загроз та зловмисника у хмарі. Так, у роботі [2] він розглядається питання довіри до провайдера, безпеки ключів, управління ризиками, безпеки хмарної архітектури, контролю доступу, захисту даних та ізоляції програм. Ця робота отримала подальший розвиток у вигляді рекомендацій NIST SP 800-144 [3]

Постановка задачі

Актуальною науково-технічною задачею в роботі є розробка методу розмежування доступу до сервісів хмарного середовища, за рахунок динамічно сформованих правил фільтрації для віртуальних брандмауерів. Для досягнення поставленої мети в роботі потрібно вирішити наступні завдання:

- ✓ розробити модель інформаційної взаємодії з врахуванням розмежування доступу в середовищі хмарних обчислень;
- ✓ вдосконалити метод динамічного формування правил фільтрації що враховує параметри віртуальних з'єднань;
- ✓ розглянути можливість використання технології блокчейн для побудови системи розмежування доступу.

Основна частина

Віртуалізація використовується в усіх хмарних середовищах. Віртуалізація - це структура або методологія поділу ресурсів одного фізичного сервера на кілька середовищ виконання шляхом застосування однієї або кількох концепцій або технологій, таких як поділ апаратного та програмного забезпечення, поділ часу, часткове або повне машинне моделювання та емуляція [4].

Віртуальну машину в неактивному стані можна визначити як набір образів жорсткого диска та метаданих, що описують конфігурацію віртуальної машини. Метадані містять інформацію про обсяг пам’яті віртуальної машини, кількість обчислювальних ядер або процесорів, фізичних мережевих інтерфейсів та інших периферійних пристроїв введення/виведення [5]. При цьому запущена віртуальна машина також має атрибути використовуваного гіпервізора, унікальний ідентифікатор і налаштування мережевого інтерфейсу. Взаємодія віртуальних машин, код яких виконується в ізольованих доменах, здійснюється по мережі. У зв'язку з цим контроль мережевої взаємодії в середовищі хмарних обчислень займає перше місце. Для функціонування мережевої підсистеми гіпервізор надає віртуальним машинам функціональність програмного мережевого мосту, який називається віртуальним комутатором, який є програмним компонентом ОС гіпервізора. При цьому, якщо необхідно забезпечити зв'язок віртуальних машин із зовнішнім світом, фізичний інтерфейс гіпервізора, який знаходиться під управлінням ОС гіпервізора, також підключається до програмного мосту. При цьому для розмежування доступу і побудови програмних компонентів гіпервізора (віртуального фаєрвола) можна використати популярну технологію блокчейн. Таким чином, взаємодія віртуальних машин в рамках одного гіпервізора здійснюється без використання фізичних ліній зв'язку і забезпечується програмним методом, наприклад за рахунок використання смарт-контрактів [6]. Відповідно, засобами контролю такого трафіку також може бути децентралізований програмний комплекс, що працює в рамках гіпервізора, або апаратно інтегрована з програмною реалізацією міжмережевого екрану.

На рисунку 1 наведено модель середовища хмарних обчислень.

Розмежування доступу як служба інформаційної безпеки нерозривно пов'язано з політикою доступу, визначає повноваження суб'єктів доступу до об'єктів і механізм, які реалізують цю політику.

Розглянемо інформаційну взаємодію хмарному середовищі. Згідно [7] для опису розмежування доступу та основних процесів, які при цьому виникають будемо використовувати поняття суб'єкта *s* та об'єкта *o*. Суб'єкт є ініціатором взаємодії, активною сутністю, і здійснює дію по відношенню до об'єкта o_2, при цьому відбувається обмін інформацією по комп'ютерній мережі.

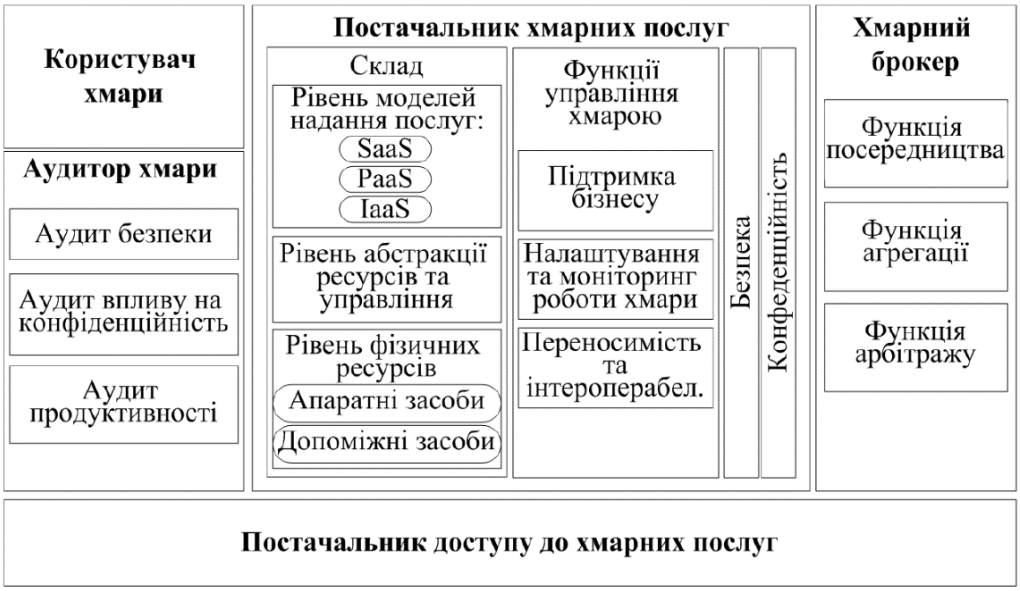

Рис. 1. Модель хмарного середовища

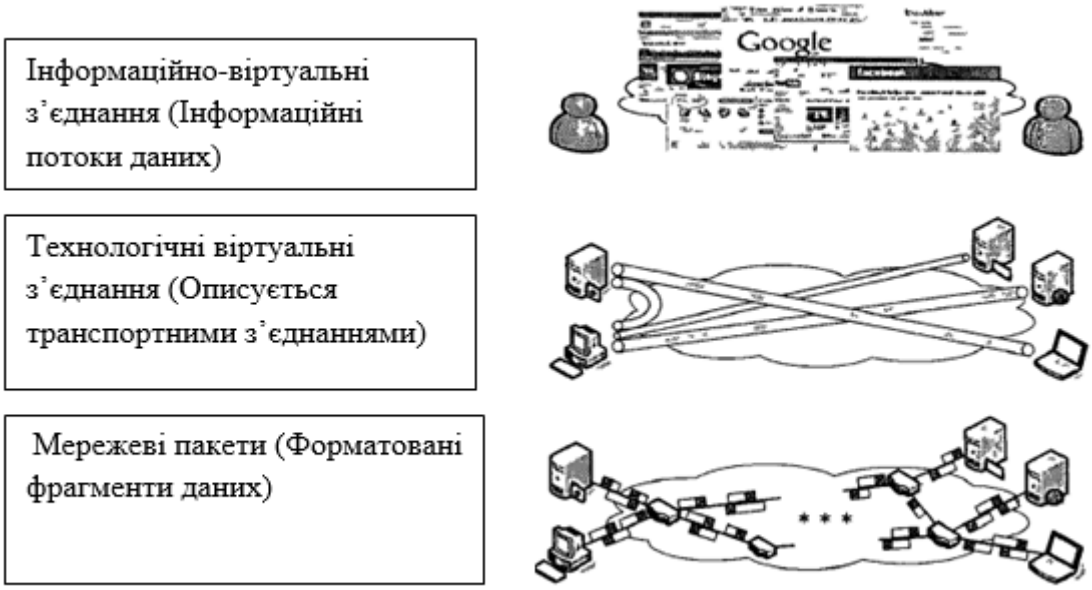

Рис. 2. Представлення інформаційної взаємодії в формі віртуального з'єднання

Для опису процесів розмежування доступу будемо використовувати рольову модель [8]. Фаєрвол формує дозвіл або заборону інформаційного віртуального з'єднання.

Наприклад, привілей може бути задано: {user:Vetal, [{transport:"TCP", port:"8080", protocol: HTTP ext:[{method:"POST"}]}]}. Таким чином формується превілей доступу до ресурсу по протоколу http з використанням методу POST по 8080 порту до віртуальних машин, що належать користувачу Vetal.

Інформаційну взаємодію в хмарному середовищі можна уявити у вигляді двох частини: підмережі віртуальних машин N_{vm}, та підмережі керування N_{man},

Кожній підмережі призначається множина IP-адрес, які можуть бути надані віртуальним машинам чи серверам.

Правила фільтрації задаються наступним чином:

$$Rul_{man}-\{rul_{mani}\}, i = \overline{1..n} \quad (1)$$

Суб'єкт та об'єкт обмінюються інформацією за допомогою моделі технологічного з'єднання та працюють з привілеями користувачів хмари, які здійснили запуск віртуальних машин [8].

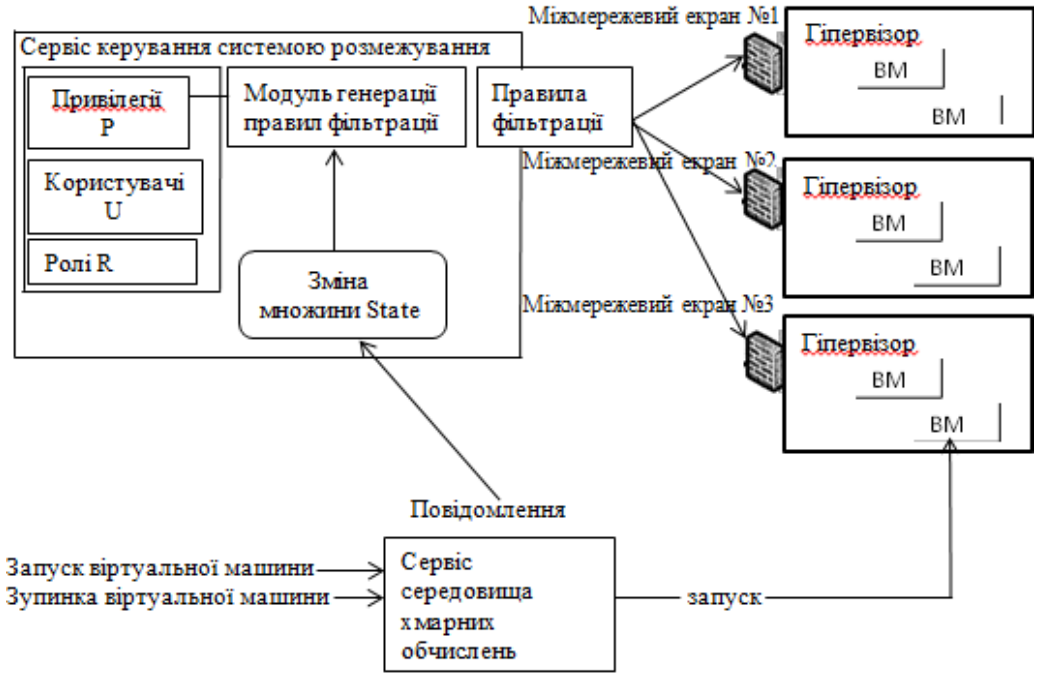

Рис. 3. Адаптивний метод конфігурації ПФ

Розглянемо можливість використання технології блокчейн для побудови системи розмежування доступу. Розподілена хеш-таблиця (словник) складається на кожному вузлі і містить відображення хеш-функцій вмісту ресурсу (унікальних ідентифікаторів та самого ресурсу). Побудову децентралізованого застосунку, децентралізований програмний комплекс, що працює в рамках гіпервізора з програмною реалізацією міжмережевого екрану доречно виконати, застосовуючи технологію блокчейна на платформі Ethereum [9]. Важливим аспектом роботи Ethereum є те, що будь-яка операція, яка виконується мережею, також одночасно виконується кожним повним вузлом [10]. Однак усі етапи обчислення на віртуальній машині Ethereum надто дорогі. Таким чином, для вирішення простих завдань (наприклад, перевірки підписів, а також інших операцій, пов'язаних з криптовалютою), смарт-контракти Ethereum можуть цілком підійти, на відміну від тих випадків, коли потрібні більш складні завдання, наприклад виконувати машиннео навчання, яке можуть спричинити надмірне використання мережі. Введення оплати запобігає діям користувача, спрямованим на зайве навантаження на мережу.

Стандартний підхід реалізований на платфомі Ethereum працює у цьому випадку нестабільно. Він полягає у тому, щоб при наступанні події P_n перерозподіляти крипто-токени та передавати їх усі разом через транзакцію CT_n Якщо виникне помилка транзакція буде скасована і може статись так, що стан контракту C залишиться незмінним. Це призведе до проблем із перерозподілом крипто-токенів у мережі M.

Альтернативний варіант, запропонований у роботі потребує керування розподілом крипто-токенів у ситуаціях, коли виникає помилка на етапівиконання транзакції CT_n і потрібно забезпечити можливість учасникам транзакції отримати свої крипто-токени рис 4.

Нехай взаємодія відбувається між смарт-контрактом C та учасниками $A_1, A_2,\ldots, A_n$. Учасники виконують транзакції $T_1, T_2,\ldots, T_n$, після яких стан розумного контракту C змінюється на проміжні стани $C', C'',\ldots, C^{(')n}$. Стани учасників відповідно змінюються на $A_1', A_2',\ldots, A_n'$. В той момент, коли в мережі M настає подія P_1, контракт C змінює свій стан на $C^{(')(n+1)}$. При цьому смарт-контракт C розподіляє крипто-токени всередині свого стану на відповідні рахунки учасників $A_1', A_2',\ldots, A_n'$. На цьому відбувається закунчення ефекту події P_1. Учасники $A_1', A_2',\ldots, A_n'$ мають можливість перевірити стан своїх акаунтів в смарт-контракті C та при потребі виконати зняття коштів через транзакції $CT_{11}, CT_{12},\ldots, CT_{1n}$. У випадку, якщо під час транзакції CT_1 виникне помилка, то учасник A_i зможе повторити транзакцію, але не може завадити іншим учасникам отримати свої крипто-токени.

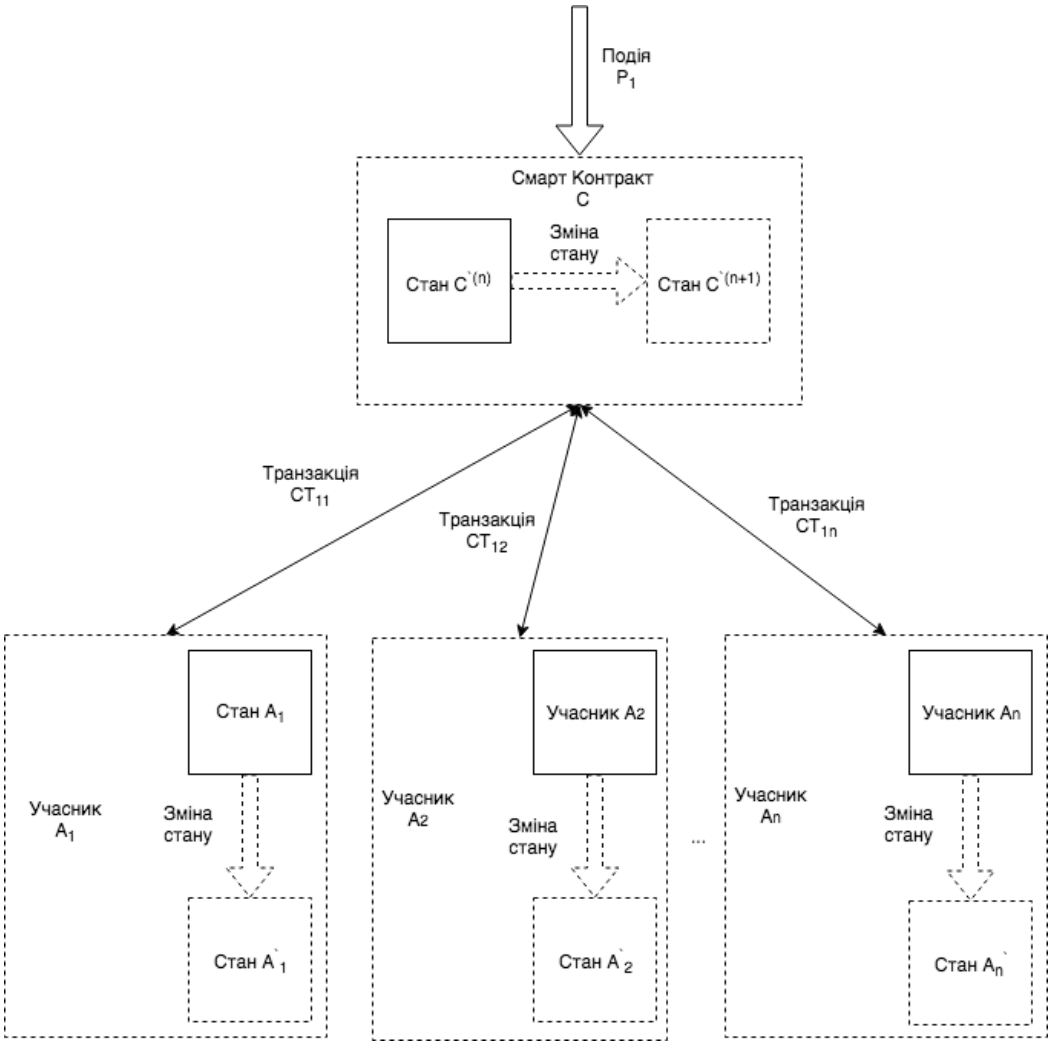

Рис. 4. Запропонований підхід до функціонування розумних контрактів

Запропонована модель може використовуватися для розподіленого виведення крипто-токенів, та дозволяє організувати процес розмежування доступу в хмарному середовищі, коли атакуючий намагається виконати транзакції T_i через власний смарт-контракт, який запрограмований на створення помилки для транзакції CT_i. Зловмисник не має можливості глобально впливати на роботу смарт-контракту C та на його стабільність для інших учасників системи блокчейн.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

На підставі опису загроз стану безпеки ресурсів хмарних обчислювальних середовищ та методів боротьби з ними виявляється, що використання стандартних підходів не дозволяє вирішити проблему підвищення рівня безпеки хмарних обчислювальних середовищ. Отже, для створення інформаційної безпеки в середовищі хмарних обчислень необхідно розробити нові методи, алгоритми, програмні продукти, які дозволять запобігти проникненню різноманітних загроз або швидко виявляти та нейтралізувати їх. Мережу блокчейн представлено системою, яка може змінювати свій стан. Така система може складатися з двох компонентів: стану системи та функції, яка її модифікує. Стан системи – це право власності на всі криптовалюти в системі. Системна функція приймає стан системи та транзакцію як аргументи. В результаті функціонування (виконання транзакцій) отримано новий стан системи, в якому відповідно зміняться права власності на криптовалюту, яка може бути використана в правилах розмежування доступу до ресурсів хмарного середовища.

Література

1. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року [Електронний ресурс]. - Режим доступу : https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text. - Назва з екрана.

2. NIST Cloud Computing Synopsis and Recommendations, SP 800-146 [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST SP800146.pdf

3. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король–Харків : Вид-во ХНЕУ, 2016. – 476 с.

4. Safe Decentralized Applications Development Using Blockchain Technologies / Viktor Cheshun, Ihor Muliar, Vasyl Yatskiv, Ruslan Shevchuk, Serhii Kulyna, Taras Tsavolyk // 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), 16-18 Sept. 2020, Deggendorf, Germany. – Publisher: IEEE, 2020. – P. 800-805.

5. Пістолюк В.О. Аналіз процесу обміну інформацією в середовищі хмарних обчислень / А.В. Джулій, Ю.П. Кльоц, І.В. Толок, О.С. Лєнков, В.О. Пістолюк // Тези доповідей XVIII Міжнародної науково-практичної конференції "Військова освіта і наука: сьогодення та майбутнє" [Текст] – К. : ВІКНУ, 2022. – 30 с.

6. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

7. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничій Центр, 2012. – 520 с.

8. David Farooq, (2019). A multi-layered blockchain framework for the smart mobility data-markets. Transportation Research Part C: Emerging Technologies. 111. 10.1016/j.trc.2020.01.002.

9. V. Yatskiv, N. Yatskiv, and O. Bandrivskyi “Proof of Video Integrity Based on Blockchain,” in Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on, 2019, pp. 431-434.

10. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “A multi-step outlier-based anomaly detection approach to network-wide traffic,” Inf. Sci. (Ny)., vol. 348, pp. 243–271, 2016

11. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп’ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

References

1. Pro skhvalennia Stratehii rozvytku sfery innovatsiinoi diialnosti na period do 2030 roku [Elektronnyi resurs]. - Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text. - Nazva z ekrana.

2. NIST Cloud Computing Synopsis and Recommendations, SP 800-146 [Elektronnyi resurs]. Rezhym dostupu: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST SP800146.pdf

3. Ostapov S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU, 2016. – 476 s.

4. Viktor Cheshun, Ihor Muliar, Vasyl Yatskiv, Ruslan Shevchuk, Serhii Kulyna, Taras Tsavolyk (2020), “Safe Decentralized Applications Development Using Blockchain Technologies”, in Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on, 2020. – pp. 800-805.

5. Pistoliuk V.O. (2022) Analiz protsesu obminu informatsiieiu v seredovyshchi khmarnykh obchyslen / A.V. Dzhulii, Yu.P. Klots, I.V. Tolok, O.S. Lienkov, V.O. Pistoliuk // Tezy dopovidei KhVIII Mizhnarodnoi naukovo-praktychnoi konferentsii "Viiskova osvita i nauka: sohodennia ta maibutnie" [Tekst] – K. : VIKNU, 2022. – 30 s.Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.

6. Dovhyi, S.O. (2012), Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuvannia /S.O. Dovhyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainskyi Vydatnychii Tsentr. – 520p.

7. David Farooq, (2019). A multi-layered blockchain framework for the smart mobility data-markets. Transportation Research Part C: Emerging Technologies. 111. 10.1016/j.trc.2020.01.002.

8. V. Yatskiv, N. Yatskiv, and O. Bandrivskyi (2019), “Proof of Video Integrity Based on Blockchain,” in Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on, 2019, pp. 431-434.

9. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “A multi-step outlier-based anomaly detection approach to network-wide traffic,” Inf. Sci. (Ny)., vol. 348, pp. 243–271, 2016

10. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №5. – pp. 22–26.

11. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, (2016), “A multi-step outlier-based anomaly detection approach to network-wide traffic,” Inf. Sci. (Ny)., vol. 348, pp. 243–271, 2016