https://doi.org/10.30857/2786-5371.2024.1.1

УДК 004.056

[1]ВАРАНІЦЬКИЙ Д. В., [1]РОЗКОЛОДЬКО О. О.,
[2]ЛЮТА М. В., [2]ЗАХАРОВА М. В., [2]ХОТУНОВ В. І.
[1]Київський національний університет технологій та дизайну, Україна
[2]Черкаський державний бізнес-коледж, Україна

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ ДАНИХ В ХМАРНИХ СЕРЕДОВИЩАХ

Мета. *Підвищення безпеки хмарних технологій. Проведення аналізу механізмів захисту інформації в хмарних середовищах, виділення їх особливостей. Пошук найбільш ефективного механізму захисту інформації, яка зберігається в хмарних середовищах. Покращення безпеки хмарних технологій дозволить користуватись такими технологіями більшій кількості людей та організацій, для яких безпека є дуже важливою. В зв'язку зі збільшенням кількості компаній та установ, що використовують хмарні середовища, для збереження та обміну внутрішніми даними виникає необхідність у покращені рівня безпеки даної системи.*

Методика. *В статті розглянуто особливості механізмів захисту даних на хмарних середовищах. Проведено їх аналіз та виділено їх головні властивості та функції. Розглянуто дані механізми та обрано найбільш ефективний.*

Результати. *Досліджено основні механізми захисту, такі як шифрування, захист даних при передачі, автентифікація та ізоляція користувачів. Виділено особливості цих механізмів. Кожен з цих механізмів має як сильні сторони, так і певні ризики втрати інформації. Для більшого розуміння принципів роботи механізмів захисту даних від загроз, представлена система демонстрації ефективності загроз на певні види даних та механізми протидій загрозам. Описані в роботі механізми захисту демонструють необхідність створення надійної системи безпеки і захисту інформації в хмарних середовищах. Використання хмарних технологій для збереження інформації обов'язково має супроводжуватися постійним вдосконаленням системи захисту, а також використанням найбільш надійного механізму.*

Наукова новизна. *Представлені механізми захисту можуть стати основою для розробки нових способів захисту інформації в хмарному середовищі, що дозволить користуватися хмарними технологіями більшій кількості людей без ризику втрати даних.*

Практична значимість. *Відповідно до результатів аналізу визначено існуючі механізми захисту даних в хмарному середовищі, порівняно механізми надання безпеки хмарним технологіям, побудови схеми взаємодії користувача, серверів управління ключами і хмарного сервера.*

Ключові слова: *хмарна технологія; захист інформації; безпека; механізм; протокол.*

Вступ. На сьогоднішній день хмарні технології є важливим засобом збереження даних, яким користується багато компаній, державні організації та просто Інтернет-користувачі. Перевагами хмарних технологій користується велика кількість людей та організацій. Сервери можуть використовуватись як для збереження особистих файлів, так і для робочих даних. Саме тому актуальною темою є забезпечення надійного захисту даних в хмарних середовищах. Покращення безпеки хмарних технологій дозволить користуватись хмарними технологіями більшій кількості людей та організацій, для яких безпека є дуже важливою. В зв'язку зі збільшенням кількості компаній та установ, що використовують хмарні середовища, для збереження та обміну внутрішніми даними виникає необхідність у покращені рівня безпеки даної системи.

Використання хмарних сервісів набуло популярності в таких установах як: провідні технологічні фірми, державні органи управління, медицина, на інші структури. Разом з таким стрімким розвитком хмарних середовищ виникають нові ризики та загрози, що призводять до некоректного функціонування сервісів, появи слабкостей в системі захисту, а також значних матеріальних втрат. Тому, використання хмарних технологій для збереження інформації

обов'язково має супроводжуватися постійним вдосконаленням системи захисту, а також використанням найбільш надійного механізму.

Проблемам захисту даних у сфері хмарних середовищ присвячені роботи Т.Г. Білової, В.О. Ярути, М.Б. Вітра [1]. Проте, якщо взяти до уваги стрімкий розвиток даної технології та рівень інформаційної злочинності в даний час, це питання потребує ефективних шляхів вирішення.

Постановка завдання. Аналіз наукових джерел по тематиці хмарних середовищ показує, що останнім часом проведено багато вдосконалень відносно безпеки зберігання даних. З кожним роком розробляються нові особливості хмарних технологій, покращується доступ, збільшується доступна для використання потужність, об'єми пам'яті та швидкість обробки інформації. Проте, ще й досі існує ряд невирішених раніше питань надійного захисту інформації хмарних серверів. В більшій мірі ці питання пов'язані з несанкціонованим доступом і витоком даних із хмарної мережі.

Результати дослідження. Відповідно вже ставши традиційними представленням, ключовими інструментальними компонентами в сучасному інформаційному середовищі є комп'ютер та мережа Інтернет, використання яких в повсякденній діяльності значно покращує життя суспільства.

Основним вектором еволюції сучасних інформаційних і комунікативних технологій є розвиток хмарних технологій. Хмарні технології – це модель надання зручного мережевого доступу до загального пула конфігурованих обчислювальних ресурсів, які можуть бути швидко представлені і звільнені з мінімальними зусиллями з управління і необхідності взаємодії з провайдером.

Існує три моделі «хмар»: програмне забезпечення, як послуга (SaaS, Software as a Service), платформа, як послуга (PaaS, Platform as a Service) та інфраструктура як послуга (IaaS, Infrastructure as a Service) [2].

Хмарні технології забезпечують швидкий доступ до різноманітних IT-послуг і скорочують затрати до рівня, відповідного фактичному використанню ресурсів. Перехід на хмарну інфраструктуру дозволяє організації швидше запускати проекти і використовувати нові можливості, збільшуючи виручку та оперативно реагуючи на зміну ринку. Перевагами хмарних сервісів є доступність, мобільність, економічність, гнучкість, висока технологічність. Завдяки цим перевагам, хмарними технологіями користується велика кількість середніх, великих компаній та навіть державні організації.

Для спільного використання ресурсів та віддаленого доступу до даних на території України існує велика кількість хмарних сервісів, серед них "Диск Google", "OneDrive", "Dropbox", "Box", "Mega", "SugarSync" та багато інших [3].

Для початку роботи з цими сервісами необхідно зареєструватись на їх сервері. Після реєстрації користувачі отримують не тільки сервіс зберігання даних з обмеженим, хоча, як правило, достатнім об'ємом дискового простору, але і відповідні додаткові хмарні сервіси.

Сервіси зберігання даних початково мали лише можливості для загрузки на сервер, зберігання та загрузки з серверу. Але з часом хмарні сервіси отримали додатковий функціонал, зв'язаний з інтелектуальною обробкою вмісту завантажених файлів.

Наприклад, можливості хмарного сервісу збереження даних "Диск Google", який надає віртуальний простір для зберігання даних, розширені за рахунок офісного пакету "Документи Google". Сервіс "Диск Google" має текстовий і табличний редактори, редактор презентацій, засоби для роботи з малюнками та графічними схемами, а також додаток для створення тестів, результати яких, як і інші файли з цього офісного пакету, будуть зберігатись в сервісі зберігання даних "Диск Google".

Вбудований пакет програм має більше обмежень, порівняно з настільними версіями програм, але має зручний для використання інтерфейс та може надавати допуск до редагування інформації відразу декільком користувачам, що покращує роботу. Також сервіс дозволяє відслідковувати зміни файлів, завдяки чому можливо вести статистику змін файлів.

Перевагами хмарних технологій користується велика кількість людей та організацій. Сервери можуть використовуватись як для збереження особистих файлів, так і для робочих даних.

Інформаційно-технічний прогрес торкнувся всіх сфер діяльності, приніс багато позитивних плодів. І, звичайно, приніс деякий фронт ризиків, пов'язаний із захистом інформації.

Для більшого розуміння принципів роботи механізмів захисту даних від загроз, представлена система, в якій демонструються механізми захисту на кожну можливу загрозу.

$$\text{Дані}(x_1, x_2, x_3, x_4 \dots x_n); \text{механізми } (m_1, m_2, m_3, m_4 \dots m_i); \text{множини } (z_1, z_2, z_3, z_4 \dots z_k),$$

де x_n – це типи даних, що знаходяться чи зберігаються на хмарному сервері;

m_i – механізми захисту інформації від загроз;

z_k – види загроз, які можуть отримати доступ, чи якимось чином пошкодити дані на сервері.

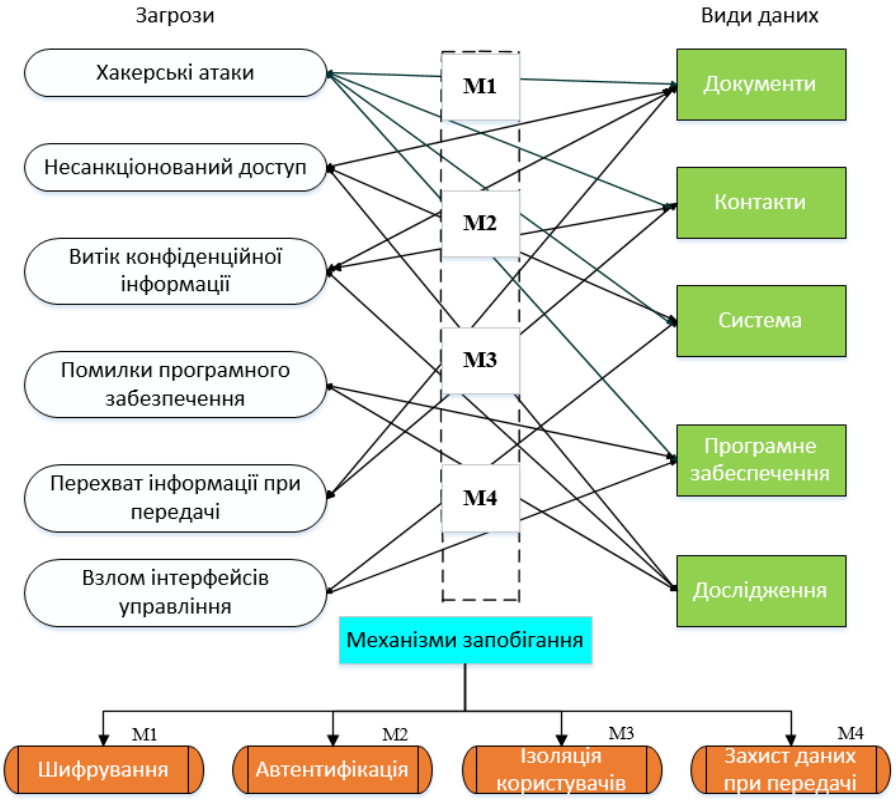

Рис. 1. **Система демонстрації ефективності загроз на певні види даних та механізми протидій загрозам**

До вище наведених загроз протидією є такі методи запобігання:

Метод шифрування буде ефективним при таких загрозах як: перехват інформації при передачі, частково при хакерських атаках та взломі інтерфейсів управління.

Метод автентифікації буде ефективним в запобіганні загрозам несанкціонованого доступу та частково при хакерських атаках.

Метод ізоляції користувачів допоможе зберегти або мінімізувати втрати даних при хакерських атаках, витоку конфіденційної інформації, помилках програмного забезпечення.

Метод захисту даних при передачі продемонструє свої переваги при перехваті інформації, при передачі, взломі інтерфейсів управління та частково при хакерських атаках.

Організаційно-технічними методами забезпечення інформаційної безпеки є: створення і вдосконалення системи забезпечення інформаційної безпеки, розробка, використання і вдосконалення засобів захисту інформації, створення систем і засобів запобігання несанкціонованого доступу до оброблюваної інформації, а також виявлення технічних пристроїв та програм, які представляють небезпеку для ефективного функціонування IT-систем [4].

Постійно зростаючі витрати на створення та експлуатацію інформаційних систем, суттєве зростання збитку від інформаційних ризиків змушують керівників шукати нові шляхи підвищення ефективності інформаційної сфери підприємств та організацій.

Найбільш ефективними механізмами безпеки хмарними технологіям є:

1. Шифрування. Один з найбільш ефективних способів збереження даних. Провайдер повинен шифрувати інформацію клієнта, яка зберігається в центрі обробки даних (ЦОД), а також в випадку відсутності необхідності – видаляти.

Зберігання ключів на хмарному сервері недоцільно, так як кожен, хто має доступ до хмарних серверів або шаблонів, міг би отримати доступ до ключа, а відтоді і до розшифрованих даних. Набір пароля при запуску системи утруднений у зв’язку з відсутністю справжньої консолі. Фізичне введення ключа замінюється запитом, який хмарний сервер відправляє зовнішньому джерелу – серверу керування ключами (Key Management Server) [5].

Вирішальним фактором для забезпечення безпеки такого рішення є роздільна експлуатація хмарного серверу та серверу управління ключами (рис. 2).

Якщо обидва розміщені у одного провайдера хмарних сервісів, то вся інформація знову виявляється зібраною в одному місці. Актуальною альтернативою є установка серверу KMS в локальному центру обміну даних(ЦОД), або в якості зовнішньої послуги в іншого сервіс-провайдера.

Якщо обидва розміщені у одного провайдера хмарних сервісів, то вся інформація знову виявляється зібраною в одному місці. Актуальною альтернативою є установка серверу KMS в локальному центру обміну даних(ЦОД), або в якості зовнішньої послуги в іншого сервіс-провайдера.

2. Захист даних при передачі. Для безпечної обробки даних, обов’язковою умовою є їх шифрована передача. В цілях захисту даних в публічній хмарі використовується тунель віртуальної приватної мережі (VPN), яка зв’язує клієнта і сервер для отримання публічних хмарних послуг.

VPN-тунель сприяє безпечним з'єднанням і дозволяє використовувати єдине ім'я і пароль для доступу до різних хмарних ресурсів. Як засіб передачі даних в публічних хмарах, VPN - з'єднання використовує загальнодоступні ресурси, такі як Інтернет. Процес заснований на режимах доступу з шифруванням за допомогою двох ключів на базі протоколу Secure Sockets Layer (SSL).

Більшість протоколів SSL і VPN в якості опції підтримують використання цифрових сертифікатів для автентифікації, за допомогою яких перевіряється ідентифікаційна інформація іншої сторони, причому ще до початку передачі даних. Такі цифрові сертифікати можуть зберігатися на віртуальних жорстких дисках в зашифрованому вигляді і використовуються вони тільки після того, як сервер управління ключами перевірить ідентифікаційну інформацію і цілісність системи [7]. Отже, такий ланцюжок дозволить передавати дані тільки тим хмарним серверам, які пройшли попередню перевірку.

Зашифровані дані при передачі повинні бути доступні тільки після автентифікації. Дані не вийде прочитати або зробити зміни в них, навіть у випадку доступу через ненадійні вузли. Такі технології досить відомі, алгоритми і надійні протоколи AES, TLS, IPsec давно використовуються провайдерами.

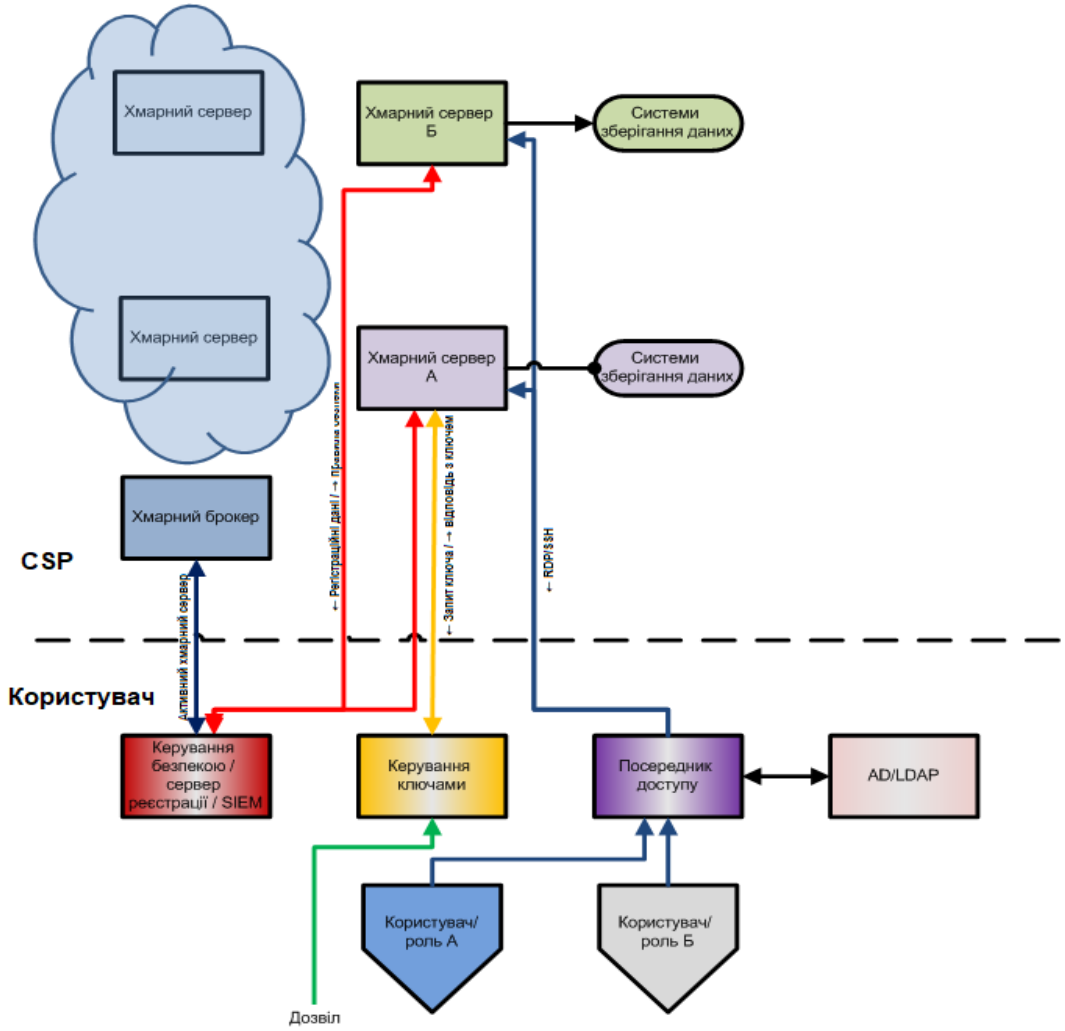

Рис. 2. **Схема взаємодії користувача, серверів управління ключами і хмарного сервера**

3. Автентифікація. Захист паролем. Для забезпечення більш високої надійності, часто використовують токени та сертифікати. Найбільш простий та достатньо надійний метод автентифікації – технологія одноразових паролів [8]. Такі паролі можуть генеруватися або спеціальними програмами, або додатковими пристроями, або сервісами с пересилкою смс-повідомлень користувачу.

Основна відмінність хмарної інфраструктури полягає у великих масштабах та широкого географічного розподілу. На перший план виходить використання для отримання одноразових паролів на мобільні пристрої, які сьогодні є практично у кожного. У найпростішому випадку одноразовий пароль буде створений спеціальним сервером автентифікації і висланий в SMS на мобільний телефон користувача після введення правильного статичного пароля на сторінку доступу до хмарного сервісу. Для прозорої взаємодії провайдера з системою ідентифікації при авторизації, також рекомендується

використовувати протокол LDAP (Lightweight Directory Access Protocol) і мову програмування SAML (Security Assertion Markup Language).

4. Ізоляція користувачів. Використання індивідуальної віртуальної машини та віртуальної мережі. Віртуальні мережі повинні бути розвернуті з застосуванням таких технологій, як VPN, VLAN та VPLS. Часто провайдери ізолюють дані користувачів одне від одного за рахунок зміни коду в єдиному програмному середовищі. Цей підхід має ризик, зв'язаний з небезпекою знайти вразливість в нестандартному коді, яка дасть доступ до даних [9]. В випадку можливої помилки в коді, користувач може отримати доступ до інформації іншого користувача.

Хмарні технології представляють значний прогрес в сфері розвитку інформаційних технологій та сервісів. В даній технології безпека грає найважливішу роль. Не дивлячись на всі складності в області безпеки, переваги таких технологій переважують можливі ризики, тому хмарні технології будуть широко затребувані на ринку інформаційних технологій [10].

Висновки. В результаті проведеного аналізу були виявлені найбільш ефективні механізми захисту інформації на хмарних сервісах. Кожен з цих механізмів має як сильні сторони, так і певні ризики втрати інформації. Описані в роботі механізми захисту демонструють необхідність створення надійної системи безпеки і захисту інформації в хмарних середовищах. Відповідно до результатів аналізу, визначено засоби нейтралізації загроз щодо забезпечення захисту даних на хмарному середовищі.

References

1. Bilova, T. G., Yaruta, V. O. (2015). Metody pidvyshchennia bezpeky obrobky danykh v khmarnykh obchyslenniakh [Methods for improving the security of data processing in cloud computing]. *Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl = Collection of scientific works of Kharkiv National University of Air Forces*, № 4 (45), P. 71–73 [in Ukrainian].

2. Ilkevich, N. S. (2021). Khmarni tekhnolohii v osviti: navchalno-metodychnyi posibnyk dlia studentiv fizyko-matematychnoho fakultetu [Cloud technologies in education: educational and methodological manual for students of the Faculty of Physics and Mathematics]. Zhytomyr: ZhDU publishing house. 88 p. [in Ukrainian].

3. Chernyak, L. (2011). Intehratsiia – osnova khmary [Integration – the basis of the cloud]. *Vidkryti systemy. SUBD = Open systems. DBMS*. September 16, 2011 [in Ukrainian].

4. Kotyashichev, I. A., Birilova, E. A. (2015). Zakhyst informatsii v "Khmarnykh tekhnolohiiakh" yak predmet natsionalnoi bezpeky [Protection of information in "Cloud technologies" as a subject of national security]. *Molodiy scientist*, No. 6.4, P. 30–34 [in Ukrainian].

5. Mell, P., Grance, T. (2011). The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology. 286 c.

6. Kuznetsov, D., Zakharova, M., Liuta, M. (2021). Criteria for evaluation of efficiency of remote administration software. *Molodiy scientist*, No. 1 (89), P. 129–133,

Література

1. Білова Т. Г., Ярута В. О. Методи підвищення безпеки обробки даних в хмарних обчисленнях. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2015. № 4 (45). С. 71–73.

2. Ількевич Н. С. Хмарні технології в освіті: навчально-методичний посібник для студентів фізико-математичного факультету. Житомир: вид-во ЖДУ, 2021. 88 с.

3. Черняк Л. Інтеграція – основа хмари. *Відкриті системи*. СУБД. 16 вересня 2011.

4. Котяшічев І. А., Бирилова Е. А. Захист інформації в "Хмарних технологіях" як предмет національної безпеки. *Молодий вчений*. 2015. № 6.4. С. 30–34.

5. Mell P., Grance T. The NIST Definition of Cloud Computing. Gaithersburg: National Institute of Standards and Technology, 2011. 286 с.

6. Kuznetsov D., Zakharova M., Liuta M. Criteria for evaluation of efficiency of remote administration software. *Молодий вчений*.

https://doi.org/10.32839/2304-5809/2021-1-89-27.

7. Tereykovskii, I. A., Korchenko, O. G., Pogorelov, V. V. (2022). Metody rozpiznavannia kiberatak: rozpiznavannia komp'iuternykh virusiv: navchalnyi posibnyk dlia zdobuvachiv stupenia bakalavr za osvitnoiu prohramoiu "Systemne prohramuvannia ta spetsializovani komp'iuterni systemy" spetsialnosti 123 Komp'iuterna inzheneriia [Methods of recognizing cyber attacks: recognition of computer viruses: study guide for bachelor's degree holders in the educational program "System programming and specialized computer systems" specialty 123 Computer engineering]. Kyiv: KPI named after Igor Sikorskyi. 127 p. [in Ukrainian].

8. Danyk, Yu. G., Vorobienko, P. P., Chernega, V. M. (2019). Fundamentals of cyber security and cyber defense: a textbook]. Second edition, revision. and additional. Odesa: ONAZ named after O. S. Popova. 320 p. [in Ukrainian].

9. Nikitchenko, V., Zakharova, M., Lyuta, M. (2019). Analiz suchasnykh system keruvannia proektamy [Analysis of modern project management systems]. *ΛΌГОΣ. Mystetstvo naukovoi dumky = ΛΌГОΣ. The art of scientific thought,* No. 3, P. 95–97. URL: https://ojs.ukrlogos.in.ua/index.php/2617-7064/issue/view/14/15 [in Ukrainian].

10. Polishchuk, D. V., Zakharova, M. V., Lyuta, M. V. (2021). Model otsinky ryzykiv informatsiinoi systemy [Information system risk assessment model]. *Suchasni elektromekhanichni ta informatsiini systemy: monohrafiia = Modern electromechanical and information systems: monograph*. By general ed. I. V. Panasyuk. Kyiv: KNUTD. P. 101–105 [in Ukrainian].

2021. № 1 (89). P. 129–133. https://doi.org/10.32839/2304-5809/2021-1-89-27.

7. Терейковський І. А., Корченко О. Г., Погорелов В. В. Методи розпізнавання кібератак: розпізнавання комп'ютерних вірусів: навчальний посібник для здобувачів ступеня бакалавр за освітньою програмою "Системне програмування та спеціалізовані комп'ютерні системи" спеціальності 123 Комп'ютерна інженерія. Київ: КПІ ім. Ігоря Сікорського, 2022. 127 с.

8. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Видання друге, перероб. та доп. Одеса: ОНАЗ ім. О.С. Попова, 2019. 320 с.

9. Нікітченко В., Захарова М., Люта М. Аналіз сучасних систем керування проектами. *ΛΌГОΣ. Мистецтво наукової думки*. 2019. № 3. С. 95–97. URL: https://ojs.ukrlogos.in.ua/index.php/2617-7064/issue/view/14/15.

10. Поліщук Д. В., Захарова М. В., Люта М. В. Модель оцінки ризиків інформаційної системи. *Сучасні електромеханічні та інформаційні системи: монографія*. За заг. ред. І. В. Панасюка. Київ: КНУТД, 2021. С. 101–105.

VARANITSKYI DMYTRO
Kyiv National University of Technologies and Design, Ukraine
E-mail: dimonstools@gmail.com

ROZKOLODKO OLEKSII
Kyiv National University of Technologies and Design, Ukraine
E-mail: rozkolodko@gmail.com

LIUTA MAIIA
Head of Software Engineering Department, Cherkasy State Business College, Ukraine
https://orcid.org/0000-0002-0248-0461
E-mail: maiialiuta@gmail.com

ZAKHAROVA MARIIA
PhD, Associate Professor of the Department of Computer Engineering and Information Technology, Cherkasy State Business College, Ukraine
https://orcid.org/0000-0001-6314-5838
Scopus Author ID: 57783473500
E-mail: zmaria17mz@gmail.com

HOTUNOV VLADISLAV
PhD, Associate Professor, Department of Computer Engineering and Information Technology, Cherkasy State Business College, Ukraine
https://orcid.org/0000-0002-2093-1270
Scopus Author ID: 57222273671
E-mail: vkhotunov@gmail.com

[1]VARANITSKYI D. V., [1]ROZKOLODKO O. O.,
[2]LIUTA M. V., [2]ZAKHAROVA M. V., [2]KHOTUNOV V. I.
[1]Kyiv National University of Technologies and Design, Ukraine
[2]Cherkasy State Business College, Ukraine

ANALYSIS OF DATA PROTECTION MECHANISMS IN CLOUD ENVIRONMENTS

Purpose: *Improving the security of cloud technologies. Analysis of information protection mechanisms in cloud environments and pointing out of their peculiarities. Searching for the most effective mechanism for protecting information, which is stored in cloud environments. Improving the security of cloud technologies will allow more people and organizations, for whom security is very important, to use such technologies. Due to the increase in the number of companies and institutions using cloud environments for the storage and exchange of internal data, there is a need for improved levels of security of this system.*

Methodology: *The article examines the peculiarities of data protection mechanisms in cloud environments. The analysis is conducted and the main properties and functions are pointed out. These mechanisms are considered and the most effective one is chosen.*

Findings: *The main mechanisms of protection, such as encryption, data protection during transmission, authentication and isolation of users, are researched. The peculiarities of these mechanisms are pointed out. Each of these mechanisms has strengths and certain risks of information loss. To better understand the principles of data protection mechanisms against dangers the system of demonstration the effectiveness of threats to certain types of data and mechanisms for counteracting dangers is presented. The protection mechanisms demonstrate the need to create a reliable system of security and protection of information in cloud environments. The use of cloud technologies for information storage must be accompanied by regular improvement of the security system, as well as the use of the most reliable mechanism.*

Scientific novelty: *The presented mechanisms of protection can be the basis for the development of new ways to protect information in the cloud environment. It will allow more people to use cloud technologies without the risk of data loss.*

Practical value: *According to the results of the analysis, the existing mechanisms for protecting data in the cloud environment are defined; the mechanisms for providing security to cloud technologies, building a scheme for user interaction, key management servers and a cloud server are compared.*

Keywords: *cloud technology; information protection; security; mechanism; protocol.*