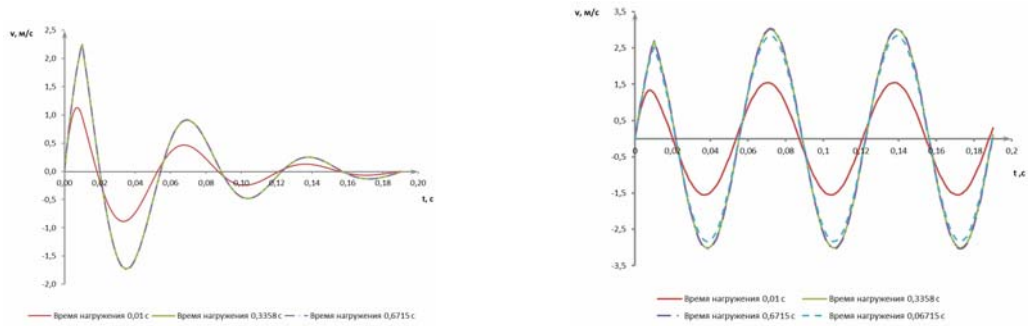

Рис. 7. Скорость движения породы при собственной частоте колебаний системы 93,57: *а* – без учета сил сопротивления, *б* с учетом сил сопротивления

Выводы. В настоящей работе предложена физическая модель разрушения кристаллической горной породы машинами ударного действия.

Горная порода представлена в виде неоднородного объекта с макроскопическими включениями, связанными различными типами прослоек.

На основе этой модели составлено дифференциальное уравнение, которое связывает силу и продолжительность удара бурового инструмента перфоратора с физико-механическими свойствами породы и скоростью ее разрушения.

Решение данного уравнения позволило получить зависимости перемещения и скорости движения горной породы, а также проанализировать влияние продолжительности нагружения на эти параметры.

Список литературы

1. **Бурильный** молоток [Электронный ресурс]. Режим доступа http://www.mining-enc.ru/b/burilnyj-molotok/

2. **Иванов, К.И.** Влияние формы ударника на коэффициент передачи энергии удара в породу [Текст] / К.И. Иванов // В сб.: «Горный породоразрушающий инструмент». – Киев: «Техника», 1970.

3. **Александров, Е.В.** Прикладная теория и расчеты ударных систем [Текст] / Е.В. Александров, В.Б**.** Соколинский. – М.: Наука, 1969. – 201 с.

4. **Шелковников, И.Г.** Использование энергии удара в процессах бурения [Текст] / И.Г. Шелковников. – Л.: Недра, 1977. – 159 с.

5. **Рудь, Ю.С.** Теория разрушения горных пород машинами ударного действия с учетом их кристаллического строения и физико-механических свойств [Текст] / Ю.С. Рудь, И.С. Радченко, С.Ю. Олейник // Гірничий вісник. – 2012. – Вип. 95 (1). – С. 112-117.

6**. Протодьяконов, М.М.** Свойства и электронное строение породообразующих минералов [Текст] / М.М. Протодьяконов. – М.: Наука, 1969. – 205 с.

Рукопись поступила в редакции 25.03.14

УДК 004.75.056.5: 004.455

В.І. МИХАЙЛІВ, аспірант, Криворізький національний університет

КРИТИЧНИЙ АНАЛІЗ ЗАСОБІВ ТА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СИСТЕМАХ ЗБЕРІГАННЯ ДАНИХ

Розглядається сучасний стан проблеми захисту інформації в хмарних системах зберігання даних, а також наводяться результати детального критичного огляду переваг та недоліків програмних засобів та методів захисту інформації в хмарних сховищах даних. Виконано аналіз найбільш значних досліджень та патентів. Розглянуто проблеми та вразливості безпеки хмарних систем зберігання даних.

Проблема та її зв'язок з науковими та практичними завданнями. Зростання кількості цілеспрямованих атак на корпоративні інфраструктури, що інтегрують хмарні середовища зберігання даних, вимагає чітко продуманої стратегії об'єднання технологій інформаційної захисту. На даний момент практично кожен з користувачів комп'ютера стикався у своїй роботі з хмарними сховищами даних та може стати потенційною жертвою загроз інформаційної безпе-

ки, що мають місце виникненню при використанні даних систем. Організація “Cloud Security Alliance” (CSA) [1] та стандарт безпеки хмарних обчислень (NIST Cloud Computing Standards Roadmap) [2] визначають базовий список атак на хмарні системи зберігання даних і список основних завдань, які повинні вирішуватися за допомогою застосування відповідних заходів:

З1 - загроза (компрометації, доступності і т.ін.) даних;

З2 - загрози, що породжуються особливостями структури і можливостями архітектури реалізації розподілених систем;

З3 - загрози неавторизованого доступу до ПЗ, даних і ресурсів;

З4 - загрози, пов’язані з некоректною моделлю загроз;

З5 - загрози, пов’язані з некоректним використанням шифрування (необхідне використання шифрування в середовищі, де існують декілька потоків даних);

З6 - загрози, пов’язані з використанням нестандартних API при розробці;

З7 - загрози віртуалізації;

З8 - загрози, що експлуатують розбіжності в глобальних політиках безпеки;

З9 - загрози, пов’язані з доступом сторонніх осіб до фізичних ресурсів або системам;

З10 - загрози, пов’язані з некоректно утилізацією (життєвий цикл) персональної інформації;

З11 - загрози, пов’язані з порушенням регіональних, національних та інтернаціональних законів, що стосуються оброблюваної інформації.

Аналіз досліджень та публікацій. Активні роботи в галузі захисту інформації систем хмарних сховищ даних ведуться такими великими компаніями як Intel, IBM, HP, Oracle, Cisco і Symantec. У табл. 1 наводяться основні класи вразливостей, сформульовані та розв’язані компаніями у своїх продуктах. Якщо питання інформаційної безпеки було вирішено повністю, воно відмічено як “+”, в разі відсутності – “–”.

Таблиця 1

Класи вразливостей хмарних сховищ даних,
сформульовані та розв’язані ІТ-компаніями у своїх продуктах

Джерело	Декларовані загрози безпеки										
	З1	З2	З3	З4	З5	З6	З7	З8	З9	З10	З11
Intel [3]	+	+	+	+	+	+	+	+	–	–	–
IBM [4]	+	+	+	+	+	–	+	–	+	+	+
Oracle [5]	+	+	+	+	–	–	+	–	–	+	–
VMware [6]	+	+	+	+	–	–	+	–	–	–	–
HP [7]	–	–	+	–	+	+	+	+	+	+	–
Symantec [8]	–	+	+	+	–	+	+	–	+	–	+
McAfee [9]	+	+	+	+	–	+	–	+	–	+	+

У табл. 2 представлено порівняльний аналіз методів різних вчених по захисту інформації в хмарних сховищах даних.

Таблиця 2

Порівняльний аналіз переваг та недоліків методів вчених по захисту інформації в хмарних сховищах даних

Метод захисту	Запропонований алгоритм	Переваги	Недоліки та обмеження
Система публічного контролю даних в сховищі [10]	Гомоморфна аутентифікація на основі РКС використовується в протоколі перевірки даних	Хеш-дерево Марклі (МНТ) керує аутентифікацію мітки блоку	Обчислювальні витрати алгоритму BLS значно менші ніж у даного методу
Метод неявного захисту он-лайн даних [11]	Алгоритм розподілу даних на частини для он-лайн збереження даних	Розділені частини даних не можуть дати яку-небудь інформацію про користувачів сервісу	У випадку, якщо користувач забув, де збережено дані, це створює труднощі для користувачів
Метод Third Party Auditing (TPA) [12]	Безпека сховища даних забезпечується з використанням алгоритму BLS	Множинний пакетний контроль даних для різних користувачів одночасно	Нездатність підтримки як публічної перевірки так і динамічної правильності даних
Аутентифікація на основі ідентифікаційних даних [13]	Новий протокол аутентифікації на основі ідентифікаційних даних, що основані на ієрархічній моделі	Легкий та більш швидкий у виконанні алгоритм	Враховано лише передачу сертифікату

Продовження табл. 2

Метод динамічного збереження даних в хмарі [14]	Нова система з використанням алгоритму протоколу зчитування даних для перевірки цілісності даних. Мульти-серверний алгоритм порівняння даних для відновлення даних	Цілісність може бути перевірена до і після запису даних	TPA не розглядається для процесу перевірки цілісності
Метод Effective and Secure Storage Protocol (ESSP) [15]	ESSP реалізується з використанням криптографії еліптичних кривих та послідовності Соболя	Динамічні операції з даними блочного рівня також використовуються для підтримки тих самих гарантій безпеки	Криптографія еліптичних кривих підходить тільки для пристроїв з обмежено малою потужністю
Метод забезпечення безпеки сховища даних SSD [16]	Універсальна та сучасна структура безпеки для різних типів хмарних сховищ. Хеш SHA, алгоритм GZIP та алгоритм SFSPL	Надано резервне копіювання даних для їх відновлення. Включає в себе основні послуги безпеки, такі як: аутентифікація, шифрування і дешифрування, а також стиснення даних	Резервні копії даних доступні на декількох серверах. Так що існує вірогідність ненадійної роботи серверів

Патенти в предметній області дослідження можна класифікувати за наступними категоріями:

засоби виявлення і запобігання розподілених мережевих атак на хмарні системи, у тому числі патенти на динамічний захист та ідентифікацію атак, підвищення автоматизації:

US 8,006,285 B1;

US 7,921,462 B2;

WO/2007/142813 та ін.;

системи забезпечення безпеки хмарних середовищ, в тому числі патенти на хмарні брандмауери, механізми обмеження використання ресурсів та валідації додатків, побудова віртуальних каналів міжмережевої взаємодії, системи агентів спостереження та хмарні антивіруси:

WO/2011/072289;

US 8,010,085;

WO/2011/010823;

US 2011083179 (A1);

CN 101827104 (A) та ін.;

системи, призначені для забезпечення безпеки хмарних середовищ, в тому числі: патенти на побудову архітектури інформаційної безпеки; системи ефективної обробки запитів та підтримки виявлення атак; системи управління доступом і надання засобів безпеки; методи, пристрої і засоби для безпечного використання мережевих ресурсів хмарних сховищ:

WO/2007/015254;

US 2007039053;

US 6,847,995;

WO/2010/030380;

US 2011219434 (A1);

US 2011072489 (A1) та ін.;

засоби для забезпечення безпеки та цілісності інформації або даних, пов'язаних з користувачем; системи, способи і пристрої, які забезпечують адміністрування та управління правилами і нормами, які регулюють захист інформації; системи і методи, що забороняють будь-які привласнення, несанкціонований доступ, фальсифікацію та розкрадання даних або зміну даних не відповідно до визначеної політики безпеки:

WO 2012035326 A1;

US 8769613 B2;

US 20140250491 A1;

US 20140137214 A1 та ін.

Постановка завдання. Метою цієї статті є аналіз недоліків сучасного стану застосування та досліджень в галузі безпеки хмарних систем зберігання даних, які підтримують конфіденційність даних через механізм контролю доступу до них, а також забезпечення цілісності даних із врахуванням відповідних нормативних і законодавчих вимог.

Викладення матеріалу та результати. Для даних в стані спокою, в даний час провайдери хмарних систем зберігання даних надають своїм користувачам два рішення: серверне шифрування і шифрування на боці клієнта.

Для серверного шифрування власник даних покладається на віддалену службу для забезпечення безпеки його даних, однак, дане рішення має два значних недоліки. Перший з них полягає в тому, що користувач буде відправляти свої конфіденційні дані в незахищеному вигляді, що робить їх вразливими для мережевих атак, коли зловмисник може використати вразливості серверів аби досягти даних користувача. В той час як другий недолік полягає в тому, що не існує жодної гарантії, що служба зашифрує дані перед їх збереженням в "хмарі".

З іншого боку, при шифруванні на боці клієнта, власник даних шифрує свої дані локально на своєму пристрої або за допомогою служби хмарного сховища, як наприклад Wuala [17] або за допомогою програмного забезпечення клієнтського шифрування, такого як TrueCrypt та BoxCryptor [18,19]. Не дивлячись на те, що дане рішення вирішує проблему, воно не охоплює всіх аспектів безпеки.

У програмному забезпеченні, такому як TrueCrypt, дані користувача шифруються за допомогою методології повного шифрування диску (FDE), що шифрує віртуальні жорсткі диски, котрі можуть монтуватися в локальну файлову систему користувача та синхронізуватися з нею. FDE ефективний при захисті конфіденційних даних в певних випадках, таких як викрадення пристроїв для резервного копіювання, проте це не проблема безпеки даних в хмарних сховищах, де фізичне викрадення пристроїв не головна проблема. Крім того, коли зашифровані дані можуть бути окремо використані серед різних користувачів, дані інструменти не допоможуть, якщо ключі шифрування не будуть сумісно розповсюджені серед користувачів по безпечному каналу передачі (або ретельно не продумано систему відкритих ключів PKI). Це явний недолік з точки зору зручності використання даних інструментів [20]. Дані рішення мають той недолік, що процес шифрування і дешифрування покладається на програмне забезпечення на основі ключів, які зберігаються на відповідному клієнтському пристрої і за деяких умов можуть бути доступні не уповноваженим особам.

З іншого боку, провайдери хмарних систем зберігання даних, які забезпечують шифрування на боці клієнта не в кращому положенні, тому що програмне забезпечення клієнта даних послуг може бути схильним до наступних загроз безпеки:

розголошення секретного ключа: клієнтське програмне забезпечення використовує ключ дешифрування, що зберігається на комп'ютері користувача для дешифрування зашифрованих даних, відправлених від провайдера хмарного сховища. Клієнтське програмне забезпечення може відправити цей ключ до провайдера або якого-небудь іншого недовіреного учасника системи;

маніпуляції з файлами: так як дані хмарні сервіси підтримують шифрування з відкритим ключем, відкриті ключі користувачів відомі іншим учасникам, включаючи провайдера. Програмне забезпечення сервера може зашифрувати шкідливий код, використовуючи відкритий ключ користувача. Користувач у свою чергу дешифрує шкідливий код, не виявивши небезпеки. Дана вразливість трапляється тому, що дані зазвичай не підписуються в даному методі;

третя загроза полягає в тому, що на боці провайдеру може бути запущений таємний агент, котрий в змозі керувати клієнтським програмним забезпеченням. Даний агент може використовуватися щоб впровадити шкідливий код в програмне забезпечення системи клієнта [21].

Навіть одна з найбезпечніших клієнтських служб хмарного сховища Wuala, що підтримує конвергентне шифрування для файлів та оптимізації збереження за допомогою де-дуплікації, має вразливість від атаки в ході якої зловмисник може ефективно підтвердити, чи володіє ціль певним файлом, шифруючи незашифрований файл, його версію, а потім просто порівнюючи вивід з файлами, що є у власності цілі, наражаючи дані користувача на небезпеку. Тому, більшість спеціалістів з безпеки радить користувачам хмарних сховищ, що для того аби їх дані зберігалися в "хмарі" без витоку конфіденційної інформації, потрібно зашифрувати дані локально, перед тим як завантажити їх у "хмару". Проте даний метод не гарантує витоку даних та секретних ключів, і це не є можливим, оскільки спричинить велике навантаження на клієнта по керуванню ключами та обслуговуванню, особливо, якщо користувач зберігає великий об'єм даних в "хмарі".

Існуючі хмарні системи зберігання даних забезпечують тільки основні механізми контролю доступу. Для перешкоджання доступу недовіреним серверам до вразливих даних, традиційні методи зазвичай покладаються на власників даних для шифрування файлів за допомогою систе-

тричного підходу ключем даних, а потім використовуючи відкритий ключ кожного користувача, щоб зашифрувати ключі даних, і тільки користувачі, що мають допустимі ключі, можуть отримати доступ до даних. Дані методи вимагають складних схем керування ключами, і власники даних повинні бути в мережі весь час, щоб відправляти ключі новому користувачу в системі. Крім того, дані методи несуть в собі значні накладні витрати, тому що сервер повинен зберігати кілька зашифрованих копій одних і тих же даних для користувачів з різними ключами.

Дана методологія не може використовуватися зі службами хмарного сховища сумісного використання, що розділяють ролі власника даних від провайдера послуг зберігання даних. Крім того, він не передбачає безпосередню взаємодію між власником даних і користувачем для надання послуги доступу до даних [22,23].

Ще однією широко поширеною методологією застосування політик контролю доступу є забезпечення керування ключами віддаленим хмарним сервером, припускаючи, що сервер є довіреним або наполовину довіреним учасником системи. Тим не менш, сервер не може бути довіреним для власників даних в хмарних сховищах і, таким чином, ці методи не можуть бути застосовані для контролю доступу для хмарних систем зберігання даних.

Висновки та напрямок подальших досліджень. Огляд основних класів вразливостей хмарної платформи дозволяє зробити висновок, що на даний час не існує готових рішень для повноцінного захисту "хмари" в силу розмаїття атак, що використовують дані вразливості.

У результаті патентного пошуку не було знайдено запатентованих інструментів захисту конфіденційності інформації в хмарних сховищах даних. Практично відсутні вітчизняні промислові розробки в галузі захисту хмарних систем зберігання даних. Є багато питань безпеки, які на сьогодні не достатньо добре проаналізовані та знаходяться ще на стадії розробки. Все це дозволяє говорити про наукову новизну та практичну значущість дослідження методів захисту інформації в хмарних системах зберігання даних.

Список літератури

1. Організація "Cloud Security Alliance" [Електронний ресурс]. – Режим доступу : https://cloudsecurityalliance.org
2. Стандарти безпеки хмарних обчислень [Електронний ресурс]. – Режим доступу : http://www.nist.gov
3. Програмні продукти компанії Intel по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.intel.com/content/www/us/en/enterprise-security/processors-with-built-in-cloud-security.html
4. Програмні продукти компанії IBM по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www-03.ibm.com/software/products/ru/network-ips
5. Програмні продукти компанії Oracle по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.oracle.com/us/solutions/cloud/managed-cloud-services/end-to-end/security-services/overview/index.html
6. Програмні продукти компанії VMware по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.vmware.com/ru/products/vcloud-network-security
7. Програмні продукти компанії HP по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www8.hp.com/ru/ru/business-solutions/solutions-index.html
8. Програмні продукти компанії Symantec по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.symantec.com/ru/ru/endpoint-protection
9. Програмні продукти компанії McAfee по захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.mcafee.com/ru/solutions/cloud-security/cloud-security.aspx
10. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing / **Q. Wang, K. Ren, W. Lou [et al.]** // IEEE Transactions on Parallel and Distributed Systems. − 2011. − № 5. – P. 847–859.
11. **Parakh A.** Online data storage using implicit security / **Abhishek Parakh, Subhash Kak** // Information Sciences. – 2009. − № 19. – P. 3323–3331.
12. Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud / **S. Balakrishnan, G. Saranya, S. Shobana [et al.]** // International Journal of Computer Science and Technology. – 2011. − № 2. – P. 397–400.
13. Identity-Based Authentication for Cloud Computing / **H. Li, Y. Dai, L. Tian [et al.]** // Cloud Computing. – 2009. − № 1. – P. 157–166.
14. **Dinesh C.** Data Integrity and Dynamic Storage Way in Cloud Computing / **C. Dinesh** // International Journal of Computer Applications. – 2011. − № 6. – P. 160−165.
15. **Syam Kumar P.** An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing / **P. Syam Kumar, R. Subramanian** // International Journal of Computer Science. – 2011. − № 6. – P. 261−274.
16. **Sajithabanu S.** Data Storage Security in Cloud / **S. Sajithabanu, E. George Prakash Raj** // International Journal of Computer Science and Technology. – 2011. − № 4. – P. 436–440.
17. Безпечна хмарна система зберігання даних Wuala [Електронний ресурс]. – Режим доступу : http://www.wuala.com

18. Клієнт TrueCrypt криптографічного захисту інформації по технології FDE в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.truecrypt.org

19. Програмне забезпечення Boxcryptor захисту інформації в хмарних системах зберігання даних [Електронний ресурс]. – Режим доступу : http://www.boxcryptor.com

20. Cloud Data Protection for the Masses / **D. Song, E. Shi, I. Fischer [et al.]** // International Journal of Computer Trends and Technology. – 2013. − № 4. – P. 701−706.

21. On the Security of Cloud Storage Services / [**Borgmann M., Hahn T., Herfert M. et al.**] ; ed. **M. Waidner**. – Darmstadt : Fraunhofer Institute for Secure Information Technology SIT, 2012. – 146 p.

22. An Efficient Attribute Based Encryption Scheme with Revocation for Outsourced Data Sharing Control / **Y. Ming, L. Fan, H. Jing-li [et al.]** // IEEE Transactions on Parallel and Distributed Systems. – 2011. − № 7. – P. 516−520.

23. A data outsourcing architecture combining cryptography and access control / **S. De Capitani di Vimercati , S. Foresti, S. Jajodia [et. al]** // ACM workshop on Computer security architecture. – 2007. − № 7. – P. 63−69.

Рукопись поступила в редакции 25.03.14

УДК 65.011.56: 622.7.01

В.С. МОРКУН, д-р техн. наук, проф.,
Н.˙В. МОРКУН, В.В. ТРОНЬ, кандидаты техн. наук, доц.,
Криворожский национальный университет

ФОРМИРОВАНИЕ РОБАСТНОГО АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ЗАМКНУТЫМ ЦИКЛОМ ИЗМЕЛЬЧЕНИЯ НА ОСНОВЕ H_∞-НОРМЫ

В статье приведены результаты исследование методов формирования автоматизированного управления технологическим процессом измельчения в условиях нестабильности характеристик железорудного сырья и неопределенности параметров технологического процесса

Ключевые слова: автоматизация, робастное управление, измельчение руд

Проблема и ее связь с научными и практическими задачами. Важность задачи синтеза регулятора и оценивания состояния объекта с учетом неопределенности в системе управления технологическим циклом измельчения в условиях изменчивости характеристик железорудного сырья и параметров технологического процесса обусловлена значительной сложностью, нелинейностью и нестационарностью объекта управления. Вследствие объективных факторов идентифицированная модель цикла измельчения отличается от реальной системы. Таким образом, необходимо исследовать методы синтеза робастного, устойчивого к неопределенности параметров, управления технологическими процессами обогащения железорудного сырья, в частности, замкнутым циклом измельчения.

Анализ исследований и публикаций. Значительное количество работ в настоящее время посвящено исследованию систем робастного управления различными техническими объектами [1].

Синтез H_2-оптимальных и H_∞-субоптимальных регуляторов скорости, обеспечивающих робастную устойчивость и качество для всех допустимых неопределенностей электропривода переменного тока на базе синхронного электродвигателя с возбуждением от постоянных магнитов, выполнен в работе [2]. Разработанная система управления функционирует в условиях неполной информации об объекте и с учетом его структурных неопределенностей.

В работе [3] на примере синтеза робастного H_∞-субоптимального регулятора скорости электропривода постоянного тока путем выбора соответствующих параметров и вида весовых функций показана возможность управления быстродействием и характером протекания переходных процессов регулируемой координаты в системе управления. Также изложены общие теоретические и инженерные рекомендации по выбору частотно-зависимых весовых функций, используемых в H_∞-теории управления для обеспечения требованиями качества переходных процессов и предоставления системе управления свойства робастности.

Решение задачи синтеза робастного регулятора для управления котельной установкой на основе метода формирования контура с ограничением на размещение полюсов передаточной функции замкнутой системы в заданной области с привлечением аппарата линейных матричных неравенств получено в работе [4]. При этом требования к системе формулируются в виде частотных ограничений на сингулярные числа передаточной функции разомкнутой системы и на размещение полюсов передаточной функции замкнутой системы в заданной области на комплексной плоскости.