http://ua.korrespondent.net/business/financial/3839343-kabmin-zberihatyme-dani-na-platformi-blokchein.

3. Технологія блокчейн. Як це працює в бізнесі [Електронний ресурс] – Режим доступу до ресурсу: http://minfin.com.ua/ua/2017/09/07/29878823/.

УДК 004.891

**Полюга Л. В.**
**Науковий керівник: к.ф.-м.н, доцент Жовтанецький М. І.**
*Львівський національний університет імені Івана Франка*

## КІБЕРБЕЗПЕКА ТА ХМАРНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

**Polyuha L.V.**

## CYBER SECURITY AND CLOUD TECHNOLOGIES IN THE ECONOMY

З ростом обізнаності і проблем, пов'язаних з хмарними обчисленнями і інформаційною безпекою, постає питання використання алгоритмів безпеки в системах даних і процесах. Оскільки інформація і процеси мігрують в хмару, питання безпеки має місце не тільки там, де виконується обчислення, але також і при джерелі інформації.

Для бізнес-користувачів можна значно скоротити витрати на обчислювання та зберігання, витрати на технічне обслуговування; для індивідуальних користувачів - зручно зберігати інформацію про розрахунок, публічні та приватні дані, а також медіа, зменшуючи кількість використання їхнього фізичного сховища та обчислювальних ресурсів.

Однією з технологій захисту приватної інформації при використанні хмарних сервісів є шифрування даних перед їх передачею у мережу, а, отже в хмару. Дані зберігаються в зашифрованому стані і для маніпуляцій з ними необхідно мати ключ для дешифрування. Оскільки до хмари можна дістатися за допомогою будь-якого пристрою, що підключений до мережі, й враховуючи те, що ці пристрої можуть не мати високої продуктивності, то виникає проблема у шифруванні інформації при обмеженості обчислювальних та часових ресурсів[1].

Постає питання у виборі належного алгоритму шифрування інформації, який би, попри свої характеристики та надійність відносно зламу, найкраще підходив для широкого використання на стороні клієнта.

У дослідженні, за допомогою програмних та теоретичних засобів проведено порівняння між алгоритмами AES, DES і Blowfish [2-4] для знаходження кращого з них з метою подальшого використання у сфері хмарних технологій, а також запропоновані алгоритми для забезпечення захисту даних хмари.

За результатами дослідження було зроблено наступні висновки:

1. Виявлено, що для алгоритму AES час шифрування зростає пропорційно до збільшення розміру ключа.

2. За результатами проведених досліджень можна стверджувати, що кібербезпека для хмарних сервісів зростає завдяки використанню алгоритму Blowfish, адже у ньому поєднується і малі затрати на час шифрування, і висока криптостійкість.

3. У наслідок комплексного порівняння досліджуваних алгоритмів шифрування за ознаками: тип шифрування, можливі набори ключів, час злому ключа методом «Повного перебору» та за загальною характеристикою безпеки; було систематизовано основні характеристики кожного з них та здійснено порівняння їх за власними обчисленнями (шифрування) за ознакою «час шифрування різного розміру файлів».

4. За результатами власних обчислень доведено, що для алгоритму Blowfish час шифрування є мінімальним незалежно від розміру файлу, проте для алгоритму AES затрати часу для шифрування є максимальними для великих файлів.

*Література:*

1. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

2. Chadi Riman, Pierre E. Abi-Char "Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey" Information Security and Computer Fraud, 2015, Vol. 3, No. 1, 1-7.

3. W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

4. Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

УДК 004.415:725.513

**Юрчук Б.О.**
**Науковий керівник: к.е.н, доцент Коляденко С.В.**
*Вінницький національний аграрний університет*

## ПОБУДОВА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЛІКАРНІ

**YURCHUK B.O.**

## CONSTRUCTION OF THE INFORMATION SYSTEM FOR A HOSPITAL

Сучасне життя неможливе без ефективного керування. Важливою категорією керування є системи обробки інформації, від яких багато в чому залежить ефективність роботи будь-якого підприємства. Дана система