

МАУП

# **ПРОБЛЕМИ МОДЕРНІЗАЦІЇ УКРАЇНИ**

Випуск 7

*Матеріали*

*Звітної науково-практичної конференції  
“Теоретико-методологічні засади та соціальна практика  
модернізації України: політичні, юридичні, економічні  
та психологічні проблеми”  
м. Київ, МАУП, 29 листопада 2018 р.*

*IV Всеукраїнської науково-практичної конференції  
“Проблеми і перспективи соціально-економічного  
розвитку України в умовах європейської інтеграції”  
м. Київ, МАУП, 14 листопада 2018 р.*

*Міжнародної наукової конференції  
“Сучасні аспекти модернізації освіти в Україні:  
стан, проблеми, тенденції розвитку”  
м. Київ, МАУП, 7 грудня 2018 р.*

Київ  
ДП “Видавничий дім “Персонал”  
2018

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом  
(протокол № 10 від 31.10.18)*

**Редакційна колегія:**

*М. Н. Курко (голова), д-р юрид. наук, проф.;  
Є. О. Романенко (заступник голови), д-р наук з держ. упр., проф.;  
А. А. Ігнатченко (відповідальний редактор), канд. техн. наук;  
І. П. Бідзюра, д-р політ. наук, проф.;  
В. М. Воронін, д-р іст. наук;  
М. Ф. Головатий, д-р політ. наук, проф.;  
А. М. Кислий, д-р юрид. наук., проф.;  
О. Л. Фещенко, канд. екон. наук, доц.;  
Л. В. Янюк (виконавчий редактор)*

*Матеріали подано в авторській редакції.  
Відповідальність за зміст та орфографію матеріалів несуть автори.*

**Проблеми модернізації України :** [зб. наук. пр.] / МАУП. — К.: ДП  
“Видавничий дім “Персонал”, 2008 —

С76 Вип. 7: Матеріали. звітн. наук.-практ. конф. “Теоретико-методологічні засади та соціальна практика модернізації України: політичні, юридичні, економічні та психологічні проблеми”, 29 листопада 2018 р.; IV Всеукр. наук.-практ. конф. “Проблеми і перспективи соціально-економічного розвитку України в умовах європейської інтеграції”, 14 листопада 2018 р.; Міжнар. наук. конф. “Сучасні аспекти модернізації освіти в Україні: стан, проблеми, тенденції розвитку”, 7 грудня 2018 р. / редкол. : М. Н. Курко (голова) [та ін.]. — 2018. — 372 с. : іл. — Бібліогр. у кінці ст.

У пропонованому збірнику подано тези учасників науково-практичних конференцій з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

**ББК 63.3(4УКР)я43+67.9(4УКР)301я43**

© Міжрегіональна Академія управління персоналом (МАУП), 2018  
© ДП “Видавничий дім “Персонал”, 2018

**Дорошенко Л. С., Лапицька Н. І.**

Удосконалення управління зайнятістю як передумова  
збереження трудового потенціалу ..... 193

**Владика Ю. П.**

Кризові явища: причини та наслідки ..... 196

**Середюк К. В.**

Методичні засади управління корпоративною соціальною відповідальністю..... 199

## **ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ**

**Домків Т. С., Чолишкіна О. Г.**

Криптоаналіз алгоритмів шифрування з використанням технології CUDA ..... 204

**Рябокін Ю. М.**

Впровадження технології блокчейн в Україні ..... 207

**Ліскін В. О.**

Онтологічний інжиніринг систем електронного навчання ..... 211

## **ІV ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ**

**“Проблеми і перспективи соціально-економічного розвитку України**

**в умовах європейської інтеграції”**

**(14 листопада 2018 р.)**

**Буковинська М. П.**

Ділова поведінка менеджера – як імпульс підвищення  
ефективності діяльності підприємств..... 215

**Братусь Г. А.**

Оцінка світової практики здійснення розрахунків  
із використанням платіжних карток..... 217

**Кобрицький В. В.**

Ризики зовнішньоекономічної діяльності та бізнес-планування ..... 220

**Козлова А. І.**

Чинники, що стоять на заваді іноземному інвестуванню в економіку України ..... 223

**Колпаков В. М.**

Проблеми людського розвитку в контексті євроінтеграційних процесів ..... 226

**Берестецька Л. М.**

Деякі аспекти використання тренінгових технологій в підготовці менеджерів ..... 230

**Головач Н. В.**

Професійна освіта як ключовий фактор розвитку трудового потенціалу України ..... 233

**Сомов Д. О.**

Взаємозв'язок організаційної культури та стратегії організації..... 237

**Бєлова А. І., Кокуба Є. М.**

Теоретичні підходи до конкурентоспроможності підприємства  
як засобу досягнення його стратегічної стійкості в умовах ринку..... 240

**Бєлова А. И., Чайкара Анил**

Целесообразность разработки бизнес-планирования продукции  
предприятия в условиях рыночной экономики ..... 244

**Т. С. ДОМКІВ**

завідувач лабораторією-полігоном кібербезпеки, ФКІТ МАУП

**О. Г. ЧОЛИШКІНА**

канд. техн. н., декан ФКІТ МАУП

## КРИПТОАНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ CUDA

Вибір необхідного ступеня захисту інформації та засобів її забезпечення є важливим завданням і повинен враховувати ряд параметрів: рівень секретності інформації; її вартість; час, протягом якого вона повинна залишатися в таємниці і т.д. Проблема захисту інформаційних ресурсів в даний час набуває все більш важливого значення.

Як відомо, далеко не всі присутні на ринку криптографічні засоби забезпечують обіцяний рівень захисту. Системи і засоби захисту інформації (СЗІ) характеризуються тим, що для них не існує простих і однозначних тестів, що дозволяють переконатися в надійному захисті інформації. Але якщо говорити про найпростіші, доступні кожному користувачеві, заходи захисту інформації, то серед них неодмінно виявиться паролний захист, який дозволяє запобігти несанкціонованому доступу до інформації.

Дані про продажі і фінансові потоки, клієнтська база даних, бухгалтерська та управлінська звітність, аналітичні звіти і прогнози – вся ця інформація необхідна як для успішного ведення операційної діяльності компанії, так і для прийняття стратегічних рішень про розвиток бізнесу. Доступ без пароля до більшої частини подібної інформації, як правило, неможливий. Така елементарна політика безпеки в будь-якій компанії.

Необхідно вирішити задачу відновлення доступу до зашифрованих даних. Чим суворіше політика безпеки, тим складніше обійти захист. Однак, в більшості випадків відновити доступ до інформації можна.

Перш за все доцільно обрати для дослідження той формат документа, який є найбільш загальноживаним [1].

На основі результатів з рис.1 для дослідження було обрано формат файлу PDF.

*Приклад тривалості підбору паролів*

У табл. 1. представлено оціночний час повного перебору паролів в залежності від їх довжини. Передбачається, що в паролі можуть використовуватися 36 різних символів (латинські літери одного регістра + цифри), а швидкість перебору складає 100 000 паролів в секунду (на *Pentium 100*) [2].

З таблиці наведеної вище можна зробити висновок, що час повного перебору паролів є занадто великим для використання на практиці, тому виникає задача мінімізації часу за допомогою розпаралелювання обчислювальних процесів.

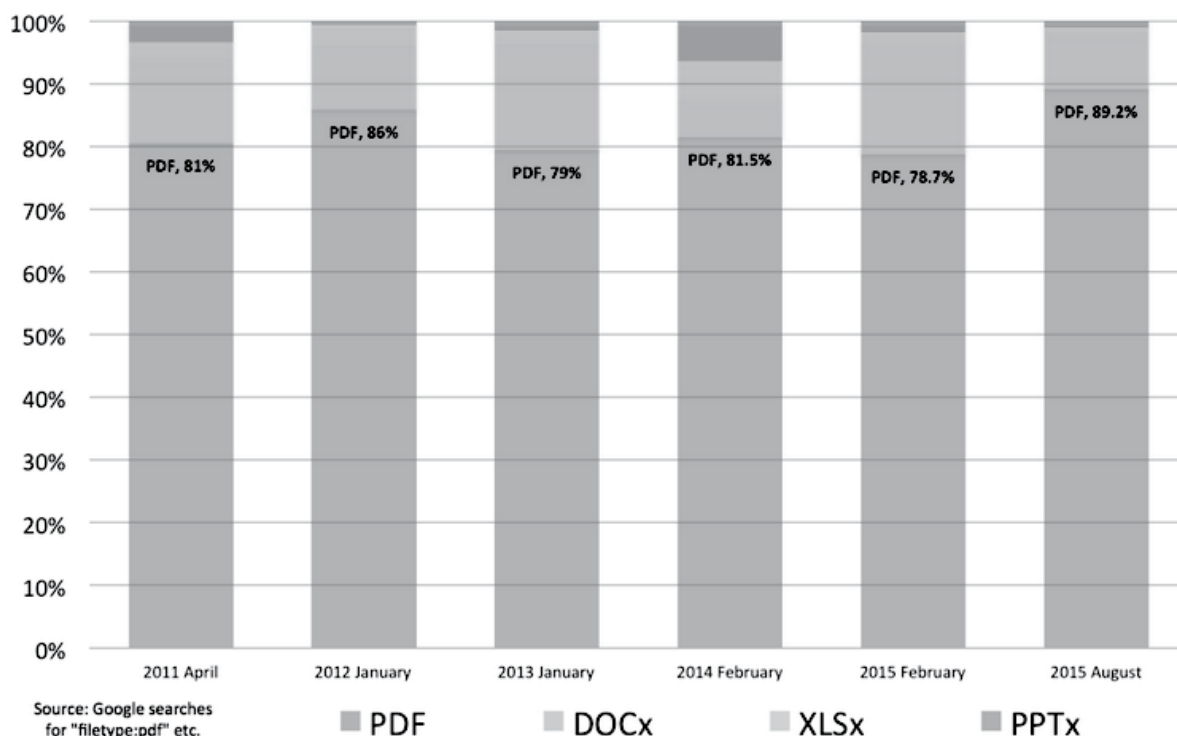


Рис. 1. Результати дослідження типів файлів для зберігання інформації

Таблиця 1

### Оціночний час повного перебору паролів

| К-сть знаків | К-сть варіантів            | Стійкість | Час перебору  |
|--------------|----------------------------|-----------|---------------|
| 2            | 1296                       | 10 біт    | < 1 сек       |
| 4            | 1 679 616                  | 21 біт    | 17 секунд     |
| 6            | 2 176 782 336              | 31 біт    | 6 годин       |
| 10           | $3,6561584 \times 10^{15}$ | 52 біта   | 1 162 роки    |
| 12           | $4,7383813 \times 10^{18}$ | 62 біта   | 1505615 років |

Розпаралелювання процесів було реалізовано за допомогою технології CUDA.

CUDA – програмно-апаратна архітектура паралельних обчислень, яка дозволяє істотно збільшити обчислювальну продуктивність завдяки використанню графічних процесорів [3].

У порівнянні з традиційним підходом до організації обчислень загального призначення за допомогою можливостей графічних API, у архітектури CUDA відзначають наступні переваги:

- Розподілена між потоками пам'ять (shared memory) розміром в 16 Кб може бути використана під організований користувачем кеш з більш широкою пропускною спроможністю, ніж при вибірці з звичайних текстур.
- Більш ефективні транзакції між пам'яттю центрального процесора і відео-пам'яттю.
- Повна апаратна підтримка цілочисельних і побітових операцій.

Отже, алгоритм повного перебору паролів з використанням технології CUDA дав такі результати, як наведено в таблиці (k – коефіцієнт швидкодії, який відображає приріст в швидкості алгоритму):

**Оціночний час повного перебору паролів  
з використанням технології CUDA**

| К-сть знаків | К-сть варіантів            | Стійкість | Час перебору | k   |
|--------------|----------------------------|-----------|--------------|-----|
| 2            | 1296                       | 10 біт    | < 1 сек      | –   |
| 4            | 1 679 616                  | 21 біт    | 5 секунд     | 3.4 |
| 6            | 2 176 782 336              | 31 біт    | 1.5 години   | 4.0 |
| 10           | $3,6561584 \times 10^{15}$ | 52 біта   | 100 днів     | 4.2 |
| 12           | $4,7383813 \times 10^{18}$ | 62 біта   | 320 років    | 4.7 |

З наведеної вище таблиці можна побачити, що використання технології розпаралелювання призвело до покращення часу роботи алгоритму, в середньому в 4 рази. Також, важливим моментом є збільшення коефіцієнту при збільшенні кількості переборів, що демонструє вигідність використання технології розпаралелювання для паролів великого розміру.

На основі матеріалу викладеного в даній роботі можна зробити висновок, що використання технології CUDA за допомогою розпаралелювання дозволяє оптимізувати алгоритми грубого перебору паролів.

Даний метод оптимізації не є найоптимальнішим, адже для більшого прискорення роботи алгоритму можна використовувати технологію CUDA в поєднанні з технологією мережевого розпаралелювання задач.

## Джерела

1. Cormac Herley. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users , 2009.
2. Скорость восстановления паролей. Електронний ресурс. Назва з екрану: [www.lockdown.co.uk](http://www.lockdown.co.uk).
3. CUDA Programming Guide. A New Architecture for Computing on the GPU. 2017. Електронний ресурс. Назва з екрану: <http://docs.nvidia.com/cuda/>