

ЗМІСТ

Вступ	3
1 Огляд.....	4
1.1 Загальний огляд та класифікація.....	4
1.2 Загальнолюдські проблеми.....	5
Висновки	7
Перелік посилань	9

ВСТУП

Проблеми, з якими людство може зіштовхнутися у майбутньому, цікавлять людину давно, а особливо — з початком НТР та швидкого прогресу соціальних, економічних та наукових аспектів життя. Письменники (особливо письменники-фантасти) часто користуються свободою творення для побудови різних варіантів розвитку людства. Як приклад можна навести цикл оповідань Айзека Азімова "Я, робот"[1], у якому автор намагається досягнути питання, які виникнуть із появою розумних машин.

Якщо звернутись до більш наукових джерел, можна теж побачити великий пласт різного ступеню підкріпленості роздумів про типи та розв'язки проблем майбутнього. Міждисциплінарну галузь, що має на меті дослідження майбутнього, називають *футурологією*. Словник Merriam-Webster [4] надає визначення футурології як науки, що розглядає майбутні можливості на основі теперішніх трендів (*переклад авт.*).

Україна теж не залишається осторонь цього процесу. Сам факт фізичного розташування нашої країни у просторово-часовому континуумі робить настання майбутнього, а разом із тим пов'язаних проблем, неминучим. Залишається лише питання конкретного вигляду цих проблем та способів їхнього розв'язання.

У даній роботі зроблено спробу огляду та систематизації українських національних проблем майбутнього.

1 ОГЛЯД

Має сенс більш детально розглянути проблеми, з якими наша нація може з деякою імовірністю зіштовхнутися у майбутньому.

1.1 Загальний огляд та класифікація

Питання, які Україні доведеться вирішувати через деякий час, природньо поділяються на два класи:

- а) Загальнолюдські проблеми
- б) Специфічно українські проблеми

Спробуємо дати класифікації підтипів, що мають місце у цих класах.

Загальнолюдські проблеми можна поділити на:

- а) Економічні:
 - Зміна структури зайнятості
 - Зростання нерівності у доходах
- б) Екологічні:
 - Зменшення біорізноманіття
 - Зміна клімату
 - Забруднення довкілля
- в) Соціальні:
 - Неоднорідна освітня модернізація
 - Масштабна урбанізація

- Гендерна нерівність
- Зростання політичного популізму

Поділ специфічних проблем для України може бути таким:

а) Економічні:

- Ресурсозалежність
- Відсутність іноваційності

б) Екологічні:

- Забруднення, зокрема гідроресурсів
- Наслідки Чорнобилю та проблема зберігання ядерних відходів
- Вичерпання лісоресурсу

в) Соціальні:

- Старіння населення та еміграція
- Застаріла освіта
- Війна з Російською Федерацією
- Внутрішня нестабільність і надмірна централізованість

Наведену класифікацію можна наочно відобразити у вигляді mind map — ієрархічного способу подання інформації [3]. Згенерована за допомогою програми SimpleMind Lite [2] така mind map наведена на рисунку 1.1.

1.2 Загальнолюдські проблеми

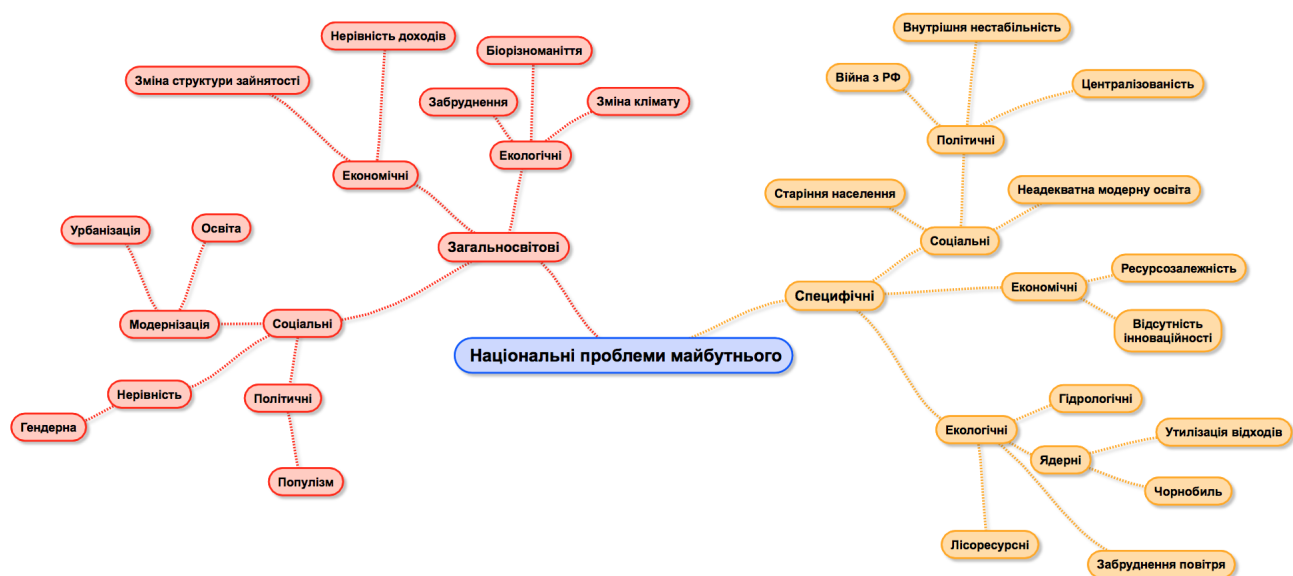


Рисунок 1.1 – Mind map

ВИСНОВКИ

У рамках виконання роботи було виконано такі завдання:

- Оглянути наявні способи обчислення дискретного логарифму у групах заданого вигляду
- Обрати оптимальний з точки зору часу роботи, простоти реалізації та здатності бути виконаним паралельно алгоритм
- Продумати архітектуру та реалізацію алгоритму
- Провести огляд сучасних платформ хмарних обчислень та обрати оптимальну.
- Провести дослідження процесу виконання реалізації на обраній платформі, визначити оптимальні параметри для запуску.
- Дослідити процес виконання з обраними параметрами. Оцінити розмір та вартість розв'язку проблеми дискретного логарифму, що можна вирішити даною реалізацією за період часу у один рік.
- Зробити висновки щодо ефективності та доцільності даного підходу до проблеми дискретного логарифму.
- Реалізувати кілька версій алгоритму, враховуючи обрану платформу.

Отримані результати свідчать про наступне:

- проблема дискретного логарифму може бути розв'язана у хмарній моделі ефективніше ніж у звичайній за рахунок паралельних обчислень
- простий варіант алгоритму *index-calculus* вимагає значних матеріальних та часових ресурсів для проблем невеликого для сучасної криптографії розміру у 160-170 біт.

Напрямами подальшого дослідження можуть бути:

- проведення аналогічної роботи для інших варіантів того самого алгоритму
- проведення аналогічної роботи для інших алгоритмів
- проведення аналогічної роботи для інших мультиплікативних груп
- дослідження інших підходів до паралелізації обчислення даної задачі у різних моделях

ПЕРЕЛІК ПОСИЛАНЬ

1. Asimov, I. I, Robot / I. Asimov. Robot series. — Bantam Books, 1950. — <https://books.google.com.ua/books?id=MD0GAQAAIAAJ>.
2. Home. — <https://simplemind.eu/>.
3. Hopper, C. Practicing College Learning Strategies / C.H. Hopper. — Cengage Learning, 2015. — <https://books.google.com.ua/books?id=JkxTCwAAQBAJ>.
4. Merriam-Webster Online. Merriam-Webster Online Dictionary. — 2017. — <http://www.merriam-webster.com>.