

**ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

О.А. Война

**ЙМОВІРНІСНІ та СТАТИСТИЧНІ
МОДЕЛІ
В ЕКОНОМІЧНИХ ДОСЛІДЖЕННЯХ**

Навчальний посібник

**Частина 2
ТЕХНОЛОГІЯ БЛОКЧЕЙН
ТА ЦИФРОВІ ГРОШІ**

Київ 2025

УДК 519.2

Рецензенти: доктор економічних наук, проф. О.І. Ляшенко,
кандидат фізико-математичних наук, доц. М.М. Шарапов

Рекомендовано до друку вченою радою факультету комп'ютерних наук та кібернетики (протокол № 14 від 20 травня 2025 року)

Ухвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики (протокол № 9 від 19 травня 2025 року)

д.ф.-м.н. Война Олександр Андрійович

Ймовірнісні та статистичні моделі в економічних дослідженнях.

Навчальний посібник. Частина 2. Технологія «блокчейн» та цифрові гроші. / О.А. Война – Київ: 2025. – 195 с.

В другій частині навчального посібника дається коротка характеристика підстав технології *блокчейн* та особливості їх реалізації в проекті криптовалюти *«Біткойн»*. Увага зосереджується також на вивченні практичних аспектів побудови економічно-математичних моделей фінансових процесів та презентації підходів до аналізу і прогнозування кон'юнктури фінансових ринків. Приведені в посібнику приклади обчислювальних методів з цієї області проілюстровані на реальних даних. Результати обчислень з використанням економічних часових рядів детально коментуються і доповнюються чіткою та конкретною предметною інтерпретацією.

Варто зауважити, що крипто-проект *«Біткойн»* – це перше практичне (в широкому масштабі) застосування технології *«Блокчейн»*. Банківська діяльність – це перший сектор економіки, в якому була застосована ця технологія, а *«біткойн»* – це перша *«програмована валюта»*, що суттєво відрізняється від всіх інших *«традиційних»* валют. Однак фінанси далеко не єдина сфера використання цієї без перебільшення революційної технології. Можливості її застосування практично необмежені.

Посібник адресований насамперед студентам, аспірантам та викладачам природничих, економічних та технічних факультетів університетів. Буде також корисним фахівцям-практикам, які користуються в своїй діяльності комп'ютерними програмами економетричного аналізу та математичної теорії прогнозу.

© Война О.А., 2025

ЗМІСТ

ЧАСТИНА 2

Технологія «блокчейн» та цифрові гроші

Розділ 3.	
Технологія блокчейн у фінансовій сфері.	5
3.1. Основні поняття пов'язані з технологією блокчейн.....	5
3.2. Централізовані та децентралізовані форми управління	11
3.3. Аналіз та прогноз коштів продукції	16
3.4. Метод найменших квадратів для нелінійної моделі: приклади та завдання для самоконтролю.	23
3.5. Метод лінеаризація для нелінійної моделі.	28
3.6. Методи передачі та захисту інформації.....	36
3.7. Транзакції в системах блокчейн та принцип «балансу».....	41
3.8. Роль криптографії та шифрування в блокчейн технології.....	47
3.9. Автентичність та консенсус в технології блокчейн.....	52
3.10. Аналітичні методи виділення тренду в часових рядах.	60
3.11. Прогнозування на основі моделі тенденції розвитку.	65
3.12. Динаміка національного доходу – лінійна модель.	69
3.13. Нелінійна модель динаміки національного доходу.	74
3.14. Передісторія створення мережі «блокчейн-біткойн».....	79
3.15. Функціонування мережі блокчейн біткойн.....	84

Розділ 4.	
Прогнозування кон'юнктури фінансових ринків	
4.1. Прогнозування на основі часового ряду.....	93
4.2. Передбачення майбутніх подій та класифікація прогнозів.	98
4.3. Прогнози на основі моделі тенденції розвитку.	103
4.4. Прогнозування курсу біткойна та гривні (лінійна модель): приклади та завдання для самоконтролю.	107
4.5. Механічні методи згладжування часових рядів.....	114
4.6. Згладжування часових рядів.....	120
4.7. «Ковзне середнє» як адаптивний метод прогнозування: приклади та завдання для самоконтролю.	125
4.8. Метод експоненціального згладжування.	131
4.9. Метод «повзучого тренду».	137
4.10. Точковий прогноз на основі «гармонічних ваг».	143
4.11. Технічний аналіз в економічних дослідженнях.....	148
4.12. «Хвильова діаграма Еліота» в технічному аналізі.....	153
4.13. Модель тенденції розвитку: точність прогнозів.	159
4.14. Прогноз динаміки національного доходу: приклади та завдання для самоконтролю.	166
4.15. Надійність економетричного прогнозу.	170
4.16. Точність прогнозів методу «повзучого тренду» : приклади та завдання для самоконтролю.	174
4.17. Деякі особливості функціонування мережі Біткойн.....	179
4.18. «Ethereum», криптовалюта «ефір» та «смарт-контракти»...	186
ЛІТЕРАТУРА.....	195

Розділ 3

Технологія блокчейн у фінансовій сфері

3.1. Основні поняття пов'язані з технологією блокчейн.

1. Суть технології блокчейн. 2. Визначення блокчейну. 3. Головні принципи блокчейну. 4. Процес функціонування блокчейн біткойна. 5. Біткойн та історія його створення.

1. Суть технології блокчейн.

Серед математичних методів прогнозування одним із основних є метод «аналогії» – коли одна і та ж формальна модель може *використовуватись* для опису багатьох можливих *явищ* абсолютно *різної природи*. Головним чином цей метод використовують для прогнозування розвитку «нових» явищ: які або *це не досліджувались* статистично-математичними методами, або *не могли досліджуватись*, оскільки раніше їх просто не існувало і не маємо емпіричних підстав для дослідження.

- Прогнозування майбутнього розвитку «нових» явищ здійснюється на основі даних про «подібні» до них явищ, на основі пошуку *загальних шляхів розвитку* досліджуваного «нового» явища з іншими, вже відомими.

Такою «суспільно-економічною *аналогією*» технології *блокчейн* цілком обґрунтовано вважається *Інтернет*.

- Поява та розвиток *блокчейну* за своїми масштабами та *динамікою розвитку* може бути порівняльною з масштабами та динамікою *розвитку* Інтернету.

Більше того, технологія блокчейн в певному сенсі є *продовженням* Інтернету.

- Якщо суспільно-економічна роль, яку зайняв в сучасному житті Інтернет – це перш за все *розповсюдження інформації*, то головна функція новітньої технології блокчейн – *це передача цінностей*.

За своєю суттю блокчейн – це технологія, яка постійно *фіксує транзакції* і робить це таким чином, що пізніше цю інформацію неможливо *стерти*. Її можна лише послідовно *оновити*, і, по суті, залишається нескінчений слід.

- Криптовалюта, криптодевізи, або цифрові гроші – це *перше* *використане* на практиці в *широкому масштабі* і тому сьогодні найбільш відоме застосування *технології блокчейна*.
- Банківська діяльність – це *перший* *здіяний сектор* використання технології блокчейн.
- *Біткойн* – це *перша* *нова цифрова валюта*, що суттєво відрізняється від всіх інших валют.

Біткойн-валюта не є втіленням жодного державного органу, банку чи компанії і працює без будь-якого центрального банку.

- *Біткойн – це програмована валюта.*

З гарантом біткойнів ви можете самі стати своїм банком.

Фінансова сфера – *перший* і один із небагатьох відомих сьогодні *способів використання* блокчейна. Однак без сумніву можливості використання цієї технології в найрізноманітніших галузях економіки та суспільства практично необмежені. Причому ці можливості будуть множитись з появою нових технологій блокчейну.

2. Визначення блокчейну.

Блокчейн має *модульну* структуру та складається з кількох частин, деякі з яких працюють *спільно*, інші – *самостійно*. Дякуючи такій модульності блокчейн має нескінчену множину варіантів можливого використання. Поширення блокчейну відбувається поступово:

- Розпочинають цей процес розробники та *стартапери*.
- Продовжують їх розробки фахівці, що пов'язані з *IT-бізнесом*.
- За ними слідує велика кількість компаній, що змогли відкрити для себе великий потенціал цієї технології.
- Далі блокчейном напевно зацікавиться широка громадськість, що буде вимагати відповідних змін.
- Цей масовий суспільний рух і зможе зрештою *змусити* до дії ті організації, що чинять спротив цим змінам.

Пояснимо більш детально, що стоїть за поняттям «блокчейн».

- Дослівно «блокчейн» означає «ланцюг блоків» (числових контейнерів), в яких зберігається найрізноманітніша інформація:
 - ✓ *транзакції,*
 - ✓ *контракти,*
 - ✓ *документи про власність,*
 - ✓ *твори мистецтва,* тощо.

Образно «блокчейн» можна порівняти з великою бухгалтерською книгою («гросбух»), що розкидана по величезній кількості комп'ютерів у всьому світі.

При цьому кожен бажаючий може вносити до неї свої записи, або читати її. Тобто:

- Блокчейн – *це програмний продукт*, що дозволяє зберігати та перетворювати інформацію.
- З одного боку – ця інформація прозора та загальнодоступна за допомогою Інтернету.
- З іншого боку – ця інформація надійно захищена.

Головною ознакою блокчейну є те, що в ньому *відсутній* центральний керуючий орган. Іншими словами:

➤ Блокчейн – це технологія реалізації транзакцій, яка завдяки використанню алгоритму *колективного консенсусу* та децентралізованого «гросбуху» створює серед всіх їх учасників атмосферу довіри, прозорості та відповідальності.

Блокчейн – це *розподілена база даних* транзакцій, де завдяки Інтернету прозоро *захищені*, автономно *зберігаються* та *перетворюються* величини і дані. Однак при цьому центральний керуючий орган *відсутній*.

Блокчейн *спирається* та використовує всі переваги і можливості Інтернету, включаючи *шифрування*.

- Кожна нова транзакція в цій базі даних *записується слідом* за попередніми, при цьому будь-яка можливість *змінити* чи *знищити* їх *виключається*.
- Система *розподілена*, тобто кожний учасник бази утворює окремий «вузол».

Вся система має *активний* характер і складена в *хронологічному* порядку. Захист від фальсифікації та перевірка відбувається за допомогою системи консенсусу та розподілу довіри:

- Кожний учасник (*вузол*) мережі володіє актуальною копією *всієї* бази даних (*гросбух*), зміст якого постійно синхронізується з усіма іншими учасниками.

3. Головні принципи блокчейну.

Підсумовуючи можемо коротко охарактеризувати блокчейн наступним чином:

- Блокчейн дозволяє автоматизувати транзакції, не залучаючи при цьому *третьої* сторони.
- Блокчейн є системою розподіленого *консенсусу* та *довіри*.
- Блокчейн це інфраструктура, що забезпечує *підтвердження справжності* даних та гарантує їх *надійний захист*.

Отже маємо можливість виділити головні принципи, на яких базується блокчейн:

1. *Розподілений* гросбух, або *регістр 2.0*, побудований за принципом *книги обліку*, що розподілена між усіма учасниками.
2. *Децентралізація* та відмова від посередництва.

Блокчейн не контролюється жодним центральним органом, в ньому панує система *довіри* у відношеннях між двома учасниками і відсутні треті особи.

3. Консенсус.

Факт прийняття транзакції чи відмови від неї є результатом *розподіленого консенсусу*, а не рішенням якоїсь централізованої інституції.

4. Незмінність та стійкість.

Неможливо змінити чи знищити записи.

5. Розподілена довіра та прозорість.

Діляться дані, операції та консенсус.

4. Процес функціонування блокчейн біткойна.

Для ілюстрації того, що потрібно для створення *блокчейну* і як він працює візьмемо приклад *блокчейн біткойна*.

Для створення і роботи *блокчейн* необхідно мати:

- *Учасників* транзакції.
- *Реєстр* (ланцюг блоків).
- *Шифрування* з ключами для захисту угоди.
- *Алгоритм* (на основі консенсусу) для *перевірки* транзакції.
- Однорангову, або децентралізовану *мережу* – комп'ютерна мережа, заснована на *рівноправності* учасників.

Схему процесу функціонування *блокчейна біткойн* розіб'ємо на *чотири* етапи:

Етап I.

Два учасника *погоджують умови* транзакції (передачу грошей, активів, фінансових документів, тощо).

Етап II.

- ✓ Журнал («*гросбух*») «*сканується*» членами мережі.
- ✓ Шляхом аналізу його хронології члени мережі *переконуються*, що *продавець* дійсно *володіє* заявленими активами чи фондами, які він продає.

Етап III.

- ✓ Якщо все відповідає дійсності, то транзакція *підтверджується*;
- ✓ *Вноситься* до журналу;
- ✓ *Додається* до останнього блоку ланцюга.

Етап IV.

Доповнений (оновлений) «*гросбух*» розповсюджується серед всіх учасників мережі.

Розповсюдженість журналу є гарантією його захищеності, тобто *незмінності та стійкості*.

Для фальсифікації транзакції необхідно було б змінити журнали всіх членів, тобто змінити чи знищити записи у всіх вузлах мережі.

- ✓ Кожна транзакція «шифрується», щоб стати одним із блоків «блокчейн біткойн»;
 - ✓ Блоки впорядковуються у ланцюг – кожна наступна транзакція «шифрується» на підставі попередньої;
- ітд.

Це й пояснює походження самої назви «блокчейн» від англійського слова «*blockchain*», що має дослівний переклад «ланцюг блоків».

Для практичної реалізації транзакції в блокчейні типу біткойн необхідно мати три «інформаційні інструменти»:

- Особистий *ключ* дебетової адреси (*біткойн-адреса*).
- Загальний *ключ* кредитової адреси.
- Суму транзакції.

Таким чином, щоб отримати статус «*достовірної*» кожна угода повинна бути *підписана* за допомогою *асиметричної криптографії*:

Відкритий ключ / Закритий ключ.

Біткойн-адреса представлена в форматі ASCII (*American Standard Code for Information Interchange* – американський стандарт коду для обміну інформації), за допомогою спеціалізованого кодування 58 буквено-цифрових символів.

- Наприклад перша створена біткойн-адреса мала вигляд:

1A1zP1eP5QGefi2DMPTfTL5SLmv7Divfna44

Біткойн-адреса – це *єдина* інформація, необхідна для отримання біткойну:

- Вистачить повідомити адресу і *платник* буде відповідати за відправлення транзакції в мережу.

5. Біткойн та історія його створення.

Як було вже підкреслено, *криптовалюта*, або *цифрові гроші* на кшталт *біткойна* – це один з перших і найбільш відомий приклад практичного використання *новітньої технології* зберігання інформації, якою є *блокчейн*. Банківська діяльність стала першим задіяним сектором, де знайшла застосування ця технологія не випадково:

- Адже це абсолютно нове, *безпечне*, *прозоре*, а що найголовніше – *децентралізоване* рішення, що дозволяє працювати з інформацією: *зберігати*, *обмінюватись*, *перевіряти* її справжність та правдивість, *поповнювати*, ітп.

Саме у *децентралізації*, тобто у *відсутності* окремої, сторонньої особи, полягає *інноваційний* характер та *оригінальність* блокчейну. Відносно невеликим коштом всі необхідні дії виконуються *самими користувачами мережі*, без участі третіх довірених осіб.

Слід зауважити, що саме з метою заміни існуючої фінансової системи був створений в 2009 р. перший блокчейн біткойн. Останні кілька років бачимо яскраві свідчення того, що банки починають усвідомлювати масштаби загрози для функціонування існуючої бізнес-моделі та приклади їх спроб використати в своїх інтересах можливості нової технології.

При цьому поле можливих застосувань технології блокчейн значно ширше і виходить далеко за межі банківської сфери.

- Термін «*біткойн*» походить від скорочення двох англійських слів:
 - ✓ bit – одиниця інформації у двійковому коді;
 - ✓ coin – монета.

Тому *біткойн* одночасно означає інформаційний протокол (*блокчейн*) мережі Інтернет та одиницю розрахунку (*біткойн*), що використовується в цій платіжній системі.

- ✓ Кожний біткойн ідентифікується в бухгалтерській книзі (*ledger*) за допомогою історії всіх угод, в яких він приймав участь з моменту його створення.

Біткойн-валюта, на відміну від інших валют, не є втіленням якоїсь офіційної інституції – державного органу, банку, корпорації, тощо. Біткойн – це нова *цифрова валюта, готівка Інтернету*.

- Технічні аспекти її створення та принципи функціонування (звичайно крім теорії програмування, адже це – *програмована валюта*) свої теоретичні корені мають в *теорії шифрування та криптографії*.
 - Асиметрична криптографія, або шифрування з *«відкритим ключем / закритим ключем»* – це *перший ключовий* принцип практичної реалізації *блокчейн-технології*.

Основною, характерною її рисою є наявність *двох ключів* шифрування, які користувач створює самостійно.

- Вперше поняття *RSA-шифрування*, або криптосистема з *відкритим ключем*, з'явилося в 1977 р. Його винахідники – Рональд Райваста, Анді Шаміра, Леонардо Адлеман, звідси скорочення RSA.
 - *Другий ключовий принцип* блокчейну – це *розподілена система*, тобто множина автономних об'єктів виконання обчислень, пов'язаних між собою в мережу (*комп'ютерів, ПК, планшетів, процесорів, ітп.*).

3.2. Централізовані та децентралізовані форми управління.

1. Математична кібернетика та блокчейн-технологія. 2. П'ять «базових стовпів» технології блокчейн. 3. «Біткойни» та «електронна готівка». 4. Децентралізація управління. 5. «Точки відмови».

1. Математична кібернетика та блокчейн-технологія.

За своєю суттю блокчейн-технологія не містить нічого принципово нового, що було б невідоме науці раніше. Цінність моделі функціонування блокчейн-мереж в наступному:

- Комбінуючи відповідним чином різноманітні *принципи, технології та знаряддя* вона дозволяє створити структуру *розподіленого зберігання даних*.

«Блокчейн» – це своєрідний, розкиданий по величезній кількості комп'ютерів у всьому світі, «*гросбух*» (щось на зразок бухгалтерської книги). На її сторінках фіксуються фінансові операції між *учасниками* системи, які утворюють окремі «*вузли*» мережі. При цьому завдяки інтегрованим до блокчейн-технології криптографічним алгоритмам, інформація, що потрапила до «*гросбуху*», не може бути ані *змінена*, ані *видалена*.

Всі наявні в ньому дані копіюються (тобто «*реплікуються*») та синхронізуються між всіма вузлами. Блокчейн дозволяє зберігати та перетворювати інформацію. Кожен бажаючий може читати цей «*гросбух*» або вносити до нього свої записи, але при цьому можна лише послідовно *обновити* вже існуючу інформацію, оскільки вона надійно захищена дякуючи математичним криптографічним інструментам

- Правила, що прийняті та обов'язкові до виконання в системі, перешкоджають проведенню «*несанкціонованих*» змін:

Навіть якщо хтось з учасників змінить дані, що зберігаються в ньому, то інші учасники системи не приймуть цього до уваги.

Сторінки умовної бухгалтерської книги називаються «*блоками*», тому дослівно «*блокчейн*» означає «*ланцюг блоків*» (числових контейнерів).

Інформація, що зберігається в цих блоках може мати найрізноманітніший характер: це можуть бути деталі *фінансових транзакцій, контракти, документи про власність, твори мистецтва*, тощо.

- Слово «*ланцюг*» в назві підкреслює ту обставину, що на відміну від «*звичайної*» бухгалтерської книги всі «*сторінки*» блокчейну жорстко з'єднані між собою дуже складними криптографічними «*замками*».

Навіть теоретично «*зламати*» їх дуже важко.

2. П'ять «базових стовпів» технології блокчейн.

Для того, щоб бути надійним сховищем даних, описана структура повинна задовольняти наступні *п'ять вимог*, які образно називають «*базовими стовпами*» блокчейн-технології.

1. Мати *децентралізовану* технологічну *основу*, в якій *відсутній* керуючий орган.

Блокчейн не контролюється жодним *центральним органом* та дозволяє автоматизувати транзакції, не залучаючи при цьому *третьої* сторони.

Блокчейн – це розподілена база даних, яка здатна розповсюджувати між всіма вузлами мережі необхідну інформацію та підтримувати її актуальний стан шляхом *реплікації та синхронізації*.

2. Мати здатність до «*хешування даних*», тобто ефективно кодувати *довільні* масиви даних в інформаційні блоки *стандартного* розміру.

3. Підтримувати нерозривний зв'язок між блоками даних.

Кожна нова транзакція в цій базі даних записується *слідом за попередніми*, при цьому будь-яка можливість змінити чи знищити їх виключається. Кожний учасник бази утворює окремий «*вузол*», а вся система складена в *хронологічному* порядку та має *активний* характер.

4. Блокчейн це інфраструктура, що гарантує *надійний захист* розміщеної в її «*блоках*» інформації, а отже використовує з цією метою виключно надійні та *стійкі* до «*зламання*» криптографічні алгоритми.

Таким чином блокчейн повинен спиратися на можливості Інтернету, використовуючи при цьому всі його переваги, включаючи, зокрема, *шифрування*.

5. Блокчейн-технологія повинна створювати серед всіх її учасників атмосферу *довіри, прозорості та відповідальності*. Все це досягається завдяки використанню алгоритму *колективного консенсусу*.

При створенні нових «*блоків*» та розміщенні в них відповідної інформації необхідно, щоб всі «*вузли*» системи виконували встановлені в ній правила. Алгоритми прийняття остаточних рішень в блокчейн-системах ґрунтуються на строго-математично доведених твердженнях з розділу «*Теорії ігор*», тому ні в кого з її членів не виникає навіть тіні сумніву в їх *легітимності*. Захист від фальсифікації та перевірка відбувається за допомогою системи *консенсусу та розподілу довіри*. Кожний учасник («*вузол*») мережі володіє актуальною копією всієї бази даних («*гросбуха*»), зміст якого постійно *синхронізується* з усіма іншими учасниками.

Це і визначає суть поняття «*колективного консенсусу*».

3. «Біткойни» та «електронна готівка».

Децентралізація та відмова від посередництва – це перший серед головних принципів, на яких базується блокчейн-технологія:

➤ Замість «системи контролю» в блокчейн-мережі панує «система довіри».

Саме у децентралізації, тобто у відсутності окремої, сторонньої особи, полягає інноваційний характер та оригінальність блокчейну. Немає сумніву в тому, що можливості застосування цієї новітньої технології в найрізноманітніших галузях економіки та суспільного життя практично необмежені.

Однак перше застосування *технології блокчейна* – це фінансова сфера. Так склалося, що поняття «біткойн» та «блокчейн» з'явилися одночасно, коли в 2009 р. з метою заміни існуючої фінансової системи був створений перший «блокчейн біткойн».

- Але ні в якому разі «біткойн» та «блокчейн» не є тотожними поняттями:
 - «Біткойн» – це крипто валюта;
 - А «блокчейн» – це *технологія* на базі якої вона реалізована.

Цифрові гроші – це тільки одна з можливих «надбудов» над структурою блокчейн, тобто одна з можливих форм *практичного використання* цієї технології.

До речі термін «криптовалюта» з'явився на два роки пізніше, ніж в обіг потрапили перші цифрові гроші.

- В 2009 р. «таємничий Сатоші Накамото» запровадив «біткойни»;
- А тільки в 2011 р. називав їх «e-cash», тобто «електронною готівкою».

4. Децентралізація управління.

Базовий принцип, що відрізняє *складну систему*, якою є *система блокчейн*, від інших складних технологічних систем, полягає в *децентралізації управління*.

- Для того, щоб будь-яка «складна система», тобто *сукупність пов'язаних між собою взаємодіючих елементів*, функціонувала та виконувала поставлені перед нею завдання, вона вимагає *управління*.

Основними способами управління складними системами в теорії вважаються *дві загальні їх форми*:

- *Централізована* форма управління;
- та
- *Децентралізована* форма управління.

При цьому:

- Не існує однозначної відповіді, яка з них є «кращою», тобто *ефективнішою*.

Існує, натомість, багато прикладів різного типу складних систем (від соціальних до технічних та технологічних), які переконливо підтверджують сформульовану тезу, і показують, що:

- Кожна з цих форма управління має свої переваги та недоліки;
- За певних обставин кожна з них може мати, як «плюси» так і «мінуси».

Як підкреслювалось, блокчейн функціонує на базі Інтернету та являється своєрідним його продовженням, а саме:

- Поширює функції та можливості Інтернету від *розповсюдження інформації до передачі цінностей*.

Тому на прикладі Інтернету проілюструємо особливості застосування кожної з форм управління, та «якість управління», яку кожна з них забезпечує.

- З одного боку – Інтернет це *децентралізована структура*.

Ця особливість знайшла своє застосування в найрізноманітніших сферах: *комерційній, соціальній, державній*, ітд.

- Однак, з іншого боку, на «нижніх» шаблях використання Інтернету, він має виразну *ієрархічну, централізовану* форму:
 - Безпосередній користувач приєднується до мережі через свого *провайдера*;
 - *Провайдер*, в свою чергу, будучи не дуже великою «*одиноцею системи*», з'єднаний одним каналом з «*більшим*» елементом мережі – *оператором*, ітд.

Закономірність тут природна та очевидна:

- *Чим крупнішим є «суб'єкт системи», тим більші його можливості в сенсі обміну інформації, як за допомогою власних каналів зв'язку, так і з використанням пунктів обміну мережевого трафіку, спільних для всіх учасників.*

5. «Точки відмови».

Однак принциповою властивістю мережі Інтернет є відсутність «*точки відмови*». Мережа побудована таким чином, що:

- «*Вимкнення*» будь-якого, навіть *найпотужнішого* елемента мережі не призведе до зупинки в *цілому* її функціонування.
- Мережа завжди *буде працювати*.

Відсутність *точок відмови* – одна з головних переваг *децентралізованих систем*.

Інакше виглядає ситуація у випадку використання «*дрібніших*» елементів мережі Інтернет, якщо розглядати їх як окремі «*складні системи*».

- Переважна більшість окремих порталів, що пропонують різноманітні он-лайн послуги, побудовано на основі *жорстко централізованої інфраструктури*.

Користаючись ними ми зіштовхуємось з головною проблемою *централізованих систем* – наявністю в них *точок відмови*:

- Якщо сервер *суб'єкта* системи, який надає послугу, вимкнутий, то доведеться чекати поки він відновить свою працездатність.

У випадку Інтернет-мережі «*Централізована систем*» автоматично передбачає наявність «*центрального серверу*», який «*керує*» контактами а системі. При цьому причини «*відмови*» можуть мати найрізноманітніший характер, що залежить від того, з яким з Інтернет-сервісів маємо справу: є це електронна пошта, чи «*хмарні*» системи зберігання даних, Інтернет-магазини або комерційна платформа, чи якийсь з сервісів, що надає фінансових послуги, система бронювання, чи адміністративний сервіс, ітп.

Натомість технологія блокчейн дає можливість уникнути небезпеки «*відмови*» при зберіганні та обміні інформацією, оскільки поняття «*центрального серверу*» в ній взагалі відсутнє.

- Будуючи *децентралізовану систему*, в якій взаємодія відбувається безпосередньо між *вузлами-клієнтами*, вона ліквідує фактор «*точки відмови*».
 - Оскільки всі вузли системи є рівноправними, а кожен з них може виконувати як функції «*споживача*» так і функції «*сервера*», то рівень надійності і працездатності *системи в цілому* підвищується практично до абсолютного рівня.

Повстає, однак, ціла низка важливих питань. Технологія блокчейн в своїй основі скерована на створення та практичне використання складних (більше того – *дуже складних*) *децентралізованих систем*. Серед передбачених до виконання цими системами завдань – це перш за все операції з *інформацією*. Не треба спеціально пояснювати наскільки *важливою* є інформація, що обертається, наприклад, в будь-якій мережі фінансової сфери. В *централізованих системах* функція адміністрування інформаційними процесами, (*переховування, перетворення, передача, розповсюдження, обмін інформацією*, тощо) покладена на «*центральный орган*». Очевидно, що в разі його відсутності реалізувати ці процеси на декілька порядків складніше.

Технологія блокчейн успішно розв'язує ці завдання. Варто однак зауважити, що на поточний момент далеко не всі проблеми, що можуть при цьому виникнути, остаточно розв'язані.

3.3. Аналіз та прогноз коштів продукції.

Економетрико-статистичні методи в дослідженні економічних процесів

1. Економетрична модель як інструмент фундаментального аналізу.
2. Глобальні кошти та глобальний об'єм продукції.
3. Кількісні показники динамічних змін.
4. Метод «аналізу механізму розвитку» явища.
5. Метод аналогії.
6. Аналітичний вигляд моделі.

1. Економетрична модель як інструмент фундаментального аналізу.

Математичні методи дослідження економічних явищ суттєво спираються та ефективно використовують в своїй структурі інструментарій і методологію сучасних розділів теорії ймовірностей та прикладної статистики.

Основним зняряддям вивчення таких явищ є *економіко-математична* їх модель, яка дозволяє провести предметний аналіз різних *факторів*, що формують досліджуване явище, вивчити *умови*, в яких ці чинники проявляються, їх *взаємодію* (чи її відсутність), *взаємозв'язки*, *взаємозалежність*, тощо.

- Без побудови та перевірки на практиці таких формальних *економіко-математичних* моделей неможливо з'ясувати суть процесів, що відбуваються в *реальній економіці*.

Одним із різновидів такого моделювання є *економетричне моделювання*.

Вивченням фінансової сфери та розробкою методів її дослідження займається окремий розділ прикладної математики. Ці методи (в «*широкому*» їх трактуванні) охоплюють проблематику від сімейного бюджету до фінансових систем окремих держав та світового фінансового ринку.

Коротку характеристику та загальну класифікацію математичних методів аналізу економічних процесів приведено в підрозділах 2.14-2.15. Цей огляд, зокрема, стосується і фінансової сфери, а також методів дослідженні кон'юнктури фінансових ринків.

Як підкреслювалось в цих підрозділах, з погляду на математичні засоби, що використовуються, та застосовану методологію дослідження, виділяють два підходи до вивчення кон'юнктури фінансових ринків:

- *Фундаментальний* аналіз;
- *Технічний* аналіз.

До фундаментального аналізу економічних процесів, включаючи питання дослідження кон'юнктури, в першу чергу зараховуються *економетричні* методи. Основним джерелом розвитку таких методів є результа-

ти досліджень великої кількості окремих дисциплін економічної науки у поєднанні із сучасними математичними та статистичними методами та широким використанням досягнень в галузі ІТ-технологій.

2. Глобальні кошти та глобальний об'єм продукції.

Особлива роль серед методів фундаментального аналізу належить економетричному моделюванню, що дозволяє будувати економіко-математичні моделі за допомогою статистичного аналізу часових рядів.

Суть економетричних методів полягають у тому, щоб спочатку вдало визначити належний аналітичний вигляд економіко-математичної моделі, яка «найбільш» адекватно описує досліджуване явище. А потім, застосовуючи ефективні методи статистичного оцінювання та спираючись на емпіричні дані, знайти числові значення параметрів формальної моделі.

Наведемо конкретний (класичний) приклад, та побудуємо економетричну модель, що описує наступне економічне явище:

- Залежність

$$K = K(Q)$$

- глобальних коштів продукції (змінна K);
- від масштабу, (загальної величини) продукції (змінна Q).

Зауважимо при цьому, що аналіз коштів продукції є одним з найважливіших аспектів господарської діяльності. Тому не випадково цією проблематикою займається окремих розділі економічної науки. В ньому досліджуються більш загальні залежності. Наприклад, моделі з великою кількістю ($k > 1$) товарів, рівень продукції ($Q_i, i = 1, 2, \dots, k$) кожного з яких впливає на загальну вартість продукції (K):

$$K = K(Q_1, Q_2, \dots, Q_k).$$

Або моделі з великою кількістю рівнянь, що відповідають великій кількості ендогенічних змінних $K = \{K_1, K_2, \dots, K_s\}$, ($s > 1$). Тобто ситуації, в якій вартість продукції є тільки однією серед взаємопов'язаних економічних величин K_1, K_2, \dots, K_s .

Варто підкреслити, що з метою уникнення небажаних в даній ситуації технічних «математичних» ускладнень, «економічні» умови прикладу максимально спрощені. Приклад, що розглядається, покликаний, щоб лише проілюструвати можливості використання математично-статистичних засобів при дослідженні фінансових процесів. Хоча не виключаємо, що отриманий результат не позбавлений також певної практичної цінності.

3. Кількісні показники динамічних змін.

В підрозділі 2.4, при побудові математичної моделі виробничої функції:

$$Q = f(X_1, X_2, \dots, X_m),$$

яка виражає *формальну* залежність між обсягом виробництва (Q) та величиною витрат необхідних для цього виробництва ресурсів (X_1, X_2, \dots, X_m), йшлося про те, яку роль при побудові формальної моделі відіграють кількісні *показники реакції* досліджуваної змінної на *можливі зміни* факторів, що її формують.

В економічному аналізі головним чином використовується *два* таких показника. Якщо $Y = F(X)$ – математичної моделі, що описує залежність між *пояснюваною* (Y) та *пояснювальною* (X) змінними моделі.

- Перший – це «*точкова еластичність залежної змінної Y відносно фактора X* »:

$$\frac{dY(X)}{dX}.$$

- Другий – це «*граничне (або маргінальне) значення залежної змінної Y по відношенню до фактора X* »:

$$\frac{dY(X)}{dX} \times \frac{X}{Y}.$$

Будемо розглядати «*одно-факторну*» залежність

$$K = K(Q)$$

глобальних коштів продукції (змінна K); від *масштабу*, (*загальної величини*) *продукції* (змінна Q).

Ключову роль в цьому випадку побудові функції $K(Q)$ відіграють наступні кількісні *показники реакції* змінної K на величину змін змінної Q :

- Маргінальні кошти продукції:

$$\frac{dK(Q)}{dQ}.$$

- Точкова еластичність коштів продукції відносно її об'єму:

$$\frac{dK(Q)}{dQ} \times \frac{Q}{K}.$$

Пояснимо трохи детальніше суть введених понять, та виведемо вказані формули для підрахунку їх значень.

Маргінальні кошти продукції:

Нехай ΔK означає приріст вартості продукції, спричинений приростом її об'єму на величину ΔQ .

Тоді відношення $\frac{\Delta K}{\Delta Q}$ вказує:

- На скільки *одиниць* зростуть (в абсолютному вимірі) кошти продукції, якщо її об'єму збільшиться на *одну одиницю*.

Якщо припустити, що величина продукції має неперервний характер, а її вартість теж змінюється неперервним чином, то *маргінальний кошт продукції* $\frac{dK(Q)}{dQ}$ визначає:

- *Зміни коштів продукції при зміні її об'єму на одну одиницю.*

Точкова еластичність коштів продукції відносно її об'єму:

Припустимо, що початковий об'єм продукції був рівний Q і зріс на величину ΔQ . Цей зріст спричинив приріст вартості продукції на величину ΔK .

Тоді відносний зріст об'єму продукції на $\frac{\Delta Q}{Q}$ процентів призво-

дить до приросту її вартості на $\frac{\Delta K}{K}$ процентів. Тому відношення $\frac{\frac{\Delta K}{K}}{\frac{\Delta Q}{Q}}$

вказує:

- На скільки процентів зростуть кошти продукції, якщо її об'єм збільшиться на *один* процент.

Цей відносний показник *реакції* змінної K на величину змін змінної Q дістав назву «*еластичність коштів продукції відносно її об'єму*».

Якщо припустити, що величина продукції має неперервний характер, а її вартість теж змінюється неперервним чином, то *точкова еластичність* $\frac{dK(Q)}{dQ} \times \frac{Q}{K}$ інформує:

- *На скільки процентів зміняться кошти продукції, якщо її об'єм збільшиться на один процент.*

Приклад 1. Маємо наступні щомісячні числові дані:

$$\{(q_t, k_t), t = 1, 2, \dots, n\},$$

що стосуються *коштів* випуску певних виробів протягом року. Тут k_t – значення в момент t змінної K , яка описує глобальну вартість продукції (*в мл.гр.*); а q_t – значення в момент t змінної Q , яка описує загальну величину продукції (*в тис. од.*).

$$\{(q_1 = 3,7; k_1 = 63), (q_2 = 3,8; k_2 = 63,3), (q_3 = 4,1; k_3 = 63,2), \\ (q_4 = 4,3; k_4 = 63,6), (q_5 = 3,5; k_5 = 62,9), (q_6 = 3,3; k_6 = 62,9), \\ (q_7 = 3,1; k_7 = 62,4), (q_8 = 2,8; k_8 = 62,3), (q_9 = 4,5; k_9 = 63,8), \\ (q_{10} = 4,7; k_{10} = 64,6), (q_{11} = 4,8; k_{11} = 65), (q_{12} = 5; k_{12} = 66,1)\}.$$

Необхідно визначити *прогноз* необхідних коштів на перший квартал наступного року, якщо плануються наступні об'єми продукції:

$$\{(q^{(mp)}_1 = 5,5), (q^{(mp)}_2 = 6,0), (q^{(mp)}_3 = 6,5)\}.$$

Побудова економетричної моделі.

4. Метод «аналізу механізму розвитку» явища. Метод «аналогії».

Будування моделі розпочинаємо від встановлення її аналітичного вигляду, тобто знайдемо «механізм» зміни коштів продукції (K) в залежності від зміни різного роду чинників: *економічних, технічних, організаційних ітп.*, що обумовлюють ті зміни.

В нашому прикладі такий чинник тільки один – її об'єм Q , тобто необхідно «вгадати» вигляд залежності:

$$K = K(Q).$$

Один із методів розв'язання цієї задачі так і називається:

- «Аналіз механізму розвитку явища».

Щоб дослідити «механізм розвитку» *глобального кошту* продукції (K), проаналізуємо спочатку динаміку зміни *одиночного кошту* продукції (k) в залежності від її об'єму.

- Одиничним коштом продукції (k) називається відношення:

$$k = \frac{K(Q)}{Q}.$$

В свою чергу, з метою вивчення *одиночного кошту* продукції (k) використовуємо метод «аналогії» та дослідимо спочатку «*обернене*» відношення $\frac{Q}{K}$. В техніці відомий такий факт:

- Для будь якого пристрою існує *оптимальний режим* його експлуатації.

Детальніше це означає наступне:

- Нехай E_G означає «*зужити*» пристроєм.
- Відповідно E_W означає енергію, яку пристрій «*виробив*» завдяки цьому.

Тоді продуктивність (η) пристрою визначає відношення:

$$\eta = \frac{E_W}{E_G}.$$

- Чим *більша* вартість η , тим *вища* продуктивність пристрою.

Досвід підтверджує наступну закономірність, яка характеризує «*механізм розвитку*» продуктивності пристрою η :

- ✓ При «*малому*» використанні пристрою (тобто коли величина E_G близька до нуля), його продуктивність η теж мала.
- ✓ Якщо E_G зростає, то зростає також і продуктивність η .
- ✓ Але після перевищення певного (оптимального для цього пристрою) «*рівня використання*», продуктивність η починає спадати.

Така «поведінка» продуктивності η є свідченням того, що пристрій *перевантажений* і діє в *несприятливих* умовах.

Якщо тепер, по «аналогії» з «умовним пристроєм»:

- Глобальні кошти продукції (K) трактувати як «зужиту» енергію E_G ;
- Об'єм продукції (Q) трактувати як «вироблену» пристроєм енергію E_W (що, зрештою є логічним);

то прийдемо до наступного висновку:

Відношення $\frac{Q}{K}$ при зростанні коштів продукції (K), «повинно» теж зростати;

Але, досягши певного «оптимального» рівня, воно почне спадати.

Повертаючись до одиничного кошту продукції:

$$k = \frac{K(Q)}{Q},$$

та враховуючи те, що (k) є «оберненою» до $\frac{Q}{K}$ величиною, спираючись на «метод аналогії», отримаємо наступну «версію» «механізму розвитку» k :

- ✓ Одиничний кошт продукції (k) при зростанні об'єму продукції Q спочатку буде спадати;
- ✓ Досягши певного «оптимального» додатного рівня, одиничний кошт продукції (k) почне зростати.

- Той найменший, «оптимальний» рівень для $k = \frac{K(Q)}{Q}$ «повинен» ві-

дповідати «оптимальному» об'ємові продукції Q , яку підприємство в стані випустити.

Маємо підстави припустити, що перевищення цього «оптимального» рівня призведе до спадку виробництва і буде свідченням того, що підприємство працює в *несприятливих* умовах.

5. Аналітичний вигляд моделі.

В практичних застосуваннях економетричних методів, зокрема на етапі пошуку аналітичного вигляду моделі, широко використовується ще один ефективний «евристичний принцип оптимальності».

Коротко його можна сформулювати наступним чином:

- ✓ Якщо функцію, що має необхідні нам властивості, не є єдиною;
- ✓ Якщо існує можливість її вибору з певної множини функцій, «подібних» з точки зору цих властивостей, тобто кожна з них має необхідні нам властивості;

✓ Якщо немає ніяких додаткових *обтунтувань*, *передумов* чи *обмежень* при виборі функції з цієї множини;

➤ То *найкращим* (з *практичної точки зору*) рішенням буде вибір «*найпростішої*» (на наш погляд) серед можливих *зної нам* функції.

Керуючись цим принципом, виразимо залежність одиничного кошту продукції від об'єму продукції Q :

$$k = \frac{K(Q)}{Q} = k(Q)$$

за допомогою *квадратної функції*:

$$K = b_0 + b_1 \cdot Q + b_2 \cdot Q^2.$$

При цьому, очевидно, необхідно подбати про те, щоб координати $(Q_0, k(Q_0))$

вершини відповідної параболи були *додатними числами*.

Враховуючи визначення «*одиничного кошту продукції $k(Q)$* », приходимо до висновку, що для формального опису глобальних коштів продукції:

$$K(Q) = Q \cdot k(Q)$$

можна використати поліном третього степеня:

$$K = a_0 + a_1 \cdot Q + a_2 \cdot Q^2 + a_3 \cdot Q^3.$$

Треба підкреслити, що статистичні дослідження реальних виробничих процесів *підтверджують* цю гіпотезу.

Зробимо ще кілька корисних практичних зауважень.

- Вільний член a_0 цього поліному треба інтерпретувати, як *сталі кошти* даного виробничого процесу, що не залежать від об'єму продукції Q .
- Продовжуючи розпочаті міркування, тобто аналізуючи *глибше* «*механізм розвитку явища*», яке вивчається, (тобто поведінку одиничного кошту продукції $k(Q)$ в цілому інтервалі зміни об'єму продукції Q) можна встановити, що цей поліном є *монотонно зростаючою функцією*.
- Причому спочатку зростає *повільно*, а починаючи від певного рівня Q , зростає *швидко*.
- Це дає можливість сформулювати певні *додаткові умови* і *обмеження* на коефіцієнти a_1 , a_2 , a_3 цього поліному.

Ці та багато інших питань детально досліджені в згаданому вже окремому, спеціальному розділі економічної науки, що займається подібною проблематикою господарської діяльності.

3.4. Метод найменших квадратів для нелінійної моделі: приклади та завдання для самоконтролю.

1. Оцінки структурних параметрів поліноміальної моделі. 2. Економетрична модель для глобальних коштів продукції. 3. Оцінки структурних параметрів. 4. Оцінка точності моделі. 5. Прогнозування на основі нелінійної економетричної моделі.

1. Оцінки структурних параметрів поліноміальної моделі.

Припустимо, що між змінними X та Y існує наступна поліноміальна залежність:

$$Y = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_K \cdot X^K.$$

Маємо можливість спостерігати ці змінні та вимірювати їх значення.

Результатом таких спостережень є наступні числові дані:

$$\{(x_t, y_t), t = 1, 2, \dots, n\}.$$

Кожна пара (x_t, y_t) – це реалізація змінної Y (координата y_t) для відповідного значення змінної X (координата x_t).

Нехай вектор

$$\hat{a}_{(k)} \approx a_{(k)}$$

означає оцінку вектора $a_{(k)}$ структурних параметрів поліноміальної моделі.

Для оцінювання структурних параметрів моделі використаємо метод найменших квадратів (МНК). Його застосування зводиться до знаходження вектора $\hat{a}_{(k)}$, що мінімізує «суму квадратів решт».

Іншими словами, введемо функціонал:

$$Q(a_{(k)}) = Q(a_0, a_1, \dots, a_K) = \sum_{t=1}^n (y_t - a_0 - a_1 \cdot x_t - a_2 \cdot x_t^2 - \dots - a_K \cdot x_t^K)^2.$$

Тоді оцінкою вектора $a_{(k)}$ структурних параметрів моделі, визначеною методом найменших квадратів (коротко «МНК-оцінкою»), буде такий вектор $\hat{a}_{(k)}$, для якого виконується співвідношення:

$$Q(\hat{a}_{(k)}) = \min_{a_{(k)}} Q(a_{(k)}).$$

Таким чином знаходження оцінки $\hat{a}_{(k)}$ вектора $a_{(k)}$ структурних параметрів моделі зводиться до мінімізації квадратичної форми $Q(a_{(k)})$.

Як відомо, $Q(a_0, a_1, \dots, a_K)$ досягає свого екстремуму в точці $\hat{a}_{(k)}$, в якій значення перших похідних $Q(a_0, a_1, \dots, a_K)$ за параметрами:

$$a_k, k = 0, 1, 2, \dots, K,$$

стають нульовими:

$$\frac{\partial Q(a_0, a_1, \dots, a_K)}{\partial a_k} = 0, k = 0, 1, 2, \dots, K.$$

Обчислимо ці похідні:

$$\frac{\partial Q(a_0, a_1, \dots, a_K)}{\partial a_0} = -2 \sum_{t=1}^n (y_t - a_0 - a_1 \cdot x_t - a_2 \cdot x_t^2 - \dots - a_K \cdot x_t^K) = 0.$$

Або:

$$\sum_{t=1}^n y_t - \sum_{t=1}^n a_0 - a_1 \sum_{t=1}^n x_t - a_2 \sum_{t=1}^n x_t^2 - \dots - a_K \sum_{t=1}^n x_t^K = 0.$$

$$\frac{\partial Q(a_0, a_1, \dots, a_K)}{\partial a_1} = -2 \sum_{t=1}^n x_t \cdot (y_t - a_0 - a_1 \cdot x_t - a_2 \cdot x_t^2 - \dots - a_K \cdot x_t^K) = 0.$$

Або:

$$\sum_{t=1}^n x_t \cdot y_t - a_0 \sum_{t=1}^n x_t - a_1 \sum_{t=1}^n x_t^2 - a_2 \sum_{t=1}^n x_t^3 - \dots - a_K \sum_{t=1}^n x_t^{K+1} = 0.$$

$$\frac{\partial Q(a_0, a_1, \dots, a_K)}{\partial a_2} = -2 \sum_{t=1}^n x_t^2 \cdot (y_t - a_0 - a_1 \cdot x_t - a_2 \cdot x_t^2 - \dots - a_K \cdot x_t^K) = 0.$$

Або:

$$\sum_{t=1}^n x_t^2 \cdot y_t - a_0 \sum_{t=1}^n x_t^2 - a_1 \sum_{t=1}^n x_t^3 - a_2 \sum_{t=1}^n x_t^4 - \dots - a_K \sum_{t=1}^n x_t^{K+2} = 0.$$

...

$$\frac{\partial Q(a_0, a_1, \dots, a_K)}{\partial a_K} = -2 \sum_{t=1}^n x_t^K \cdot (y_t - a_0 - a_1 \cdot x_t - a_2 \cdot x_t^2 - \dots - a_K \cdot x_t^K) = 0.$$

Або:

$$\sum_{t=1}^n x_t^K \cdot y_t - a_0 \sum_{t=1}^n x_t^K - a_1 \sum_{t=1}^n x_t^{K+1} - a_2 \sum_{t=1}^n x_t^{K+2} - \dots - a_K \sum_{t=1}^n x_t^{K+K} = 0.$$

Введемо наступні позначення:

$$c_k = \sum_{t=1}^n (x_t)^k, \quad k = 0, 1, 2, \dots, 2K;$$

$$b_k = \sum_{t=1}^n y_t \cdot (x_t)^k, \quad k = 0, 1, 2, \dots, K.$$

Побудуємо матрицю **C** та вектор **B** наступним чином:

$$\mathbf{C} = \begin{bmatrix} c_0 & c_1 & \dots & c_K \\ c_1 & c_2 & \dots & c_{K+1} \\ \vdots & \vdots & \dots & \vdots \\ c_K & c_{K+1} & c_{K+2} & c_{2K} \end{bmatrix}; \quad \mathbf{B} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_K \end{bmatrix}.$$

Нехай

$$\mathbf{a}^*_{(k)} = \{a^*_0, a^*_1, a^*_2, \dots, a^*_K\}^T$$

позначає вектор-стовпчик, складений з МНК-оцінок вектора $a_{(k)}$ структурних параметрів моделі. Тут символ $(^T)$ означає операцію транспонування.

Тоді числові значення цих оцінок визначаємо, як розв'язки наступної системи рівнянь (в математичній статистиці цю систему називають «нормальною системою рівнянь»):

$$\mathbf{C} \cdot \mathbf{a}^*_{(k)} = \mathbf{B},$$

або

$$\mathbf{a}^*_{(k)} = \mathbf{C}^{-1} \cdot \mathbf{B}.$$

2. Економетрична модель для глобальних коштів продукції.

Повернемось до сформульованого в підрозділі 3.3 прикладу 1.

Приклад 1. Маємо наступні щомісячні числові дані:

$$\{(q_t, k_t), t = 1, 2, \dots, n\},$$

що стосуються коштів випуску певних виробів протягом року.

- k_t – значення в момент t змінної K , яка описує глобальну вартість продукції (в мл.гр.);
- q_t – значення в момент t змінної Q , яка описує загальну величину продукції (в тис. од.).

$$\{(q_1 = 3,7; k_1 = 63), (q_2 = 3,8; k_2 = 63,3), (q_3 = 4,1; k_3 = 63,2), \\ (q_4 = 4,3; k_4 = 63,6), (q_5 = 3,5; k_5 = 62,9), (q_6 = 3,3; k_6 = 62,9), \\ (q_7 = 3,1; k_7 = 62,4), (q_8 = 2,8; k_8 = 62,3), (q_9 = 4,5; k_9 = 63,8), \\ (q_{10} = 4,7; k_{10} = 64,6), (q_{11} = 4,8; k_{11} = 65), (q_{12} = 5; k_{12} = 66,1)\}.$$

Припускаємо, що залежність між глобальними коштами продукції (K) та глобальним об'ємом продукції (Q) має наступний вигляд:

$$K = a_0 + a_1 \cdot Q + a_2 \cdot Q^2 + a_3 \cdot Q^3.$$

Необхідно визначити прогноз $\{k^{(np)}_1, k^{(np)}_2, k^{(np)}_3\}$ необхідних коштів на перший квартал наступного року, якщо плануються наступні об'єми продукції:

$$\{(q^{(np)}_1 = 5,1), (q^{(np)}_2 = 5,2), (q^{(np)}_3 = 5,4)\}.$$

Завдання 1. Виконати в аркуші «Excel». наступні розрахунки:

- Використовуючи числові дані $\{(q_t, k_t), t = 1, 2, \dots, n\}$, що стосуються коштів випуску певних виробів протягом року, підрахувати наступні числа: $\{c_0, c_1, \dots, c_5, c_6\}$, та $\{b_0, b_1, b_2, b_3\}$, де

$$c_l = \sum_{t=1}^n (q_t)^l, l = 0, 1, \dots, 6; \text{ та } b_l = \sum_{t=1}^n k_t \cdot (q_t)^l, l = 0, 1, 2, 3.$$

Відповідь:

$$c_0 = 12; c_1 = 47,6; c_2 = 194,4; c_3 = 815,048; c_4 = 3496,73; \\ c_5 = 15301,1766; c_6 = 68085,82908. \\ b_0 = 763,1; b_1 = 3035,06; b_2 = 12427,544; b_3 = 52232,5526;$$

3 Оцінки структурних параметрів.

Завдання 2. Застосовуючи *Метод Найменших Квадратів* безпосередньо до нелінійної моделі у вигляді полінома третьої степені, побудувати *статистичні оцінки* для *структурних параметрів* моделі $\{a_0, a_1, a_2, a_3\}$.

Розв'язок. Вектор-стовпчик

$$\mathbf{a}^{*(k)} = \{a^*_{0}, a^*_{1}, a^*_{2}, a^*_{3}\}^T,$$

складений з числових значення *оцінок структурних параметрів* моделі визначаємо за формулою:

$$\mathbf{a}^{*(k)} = \mathbf{C}^{-1} \cdot \mathbf{B},$$

де

$$\mathbf{C} = \begin{bmatrix} c_0 & c_1 & c_2 & c_3 \\ c_1 & c_2 & c_3 & c_4 \\ c_2 & c_3 & c_4 & c_5 \\ c_3 & c_4 & c_5 & c_6 \end{bmatrix}; \mathbf{B} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix},$$

Відповідь: $a^*_0 = 16,564$; $a^*_1 = 37,859$; $a^*_2 = -10,388$; $a^*_3 = 0,9591$.

Завдання 3. Знайти числове значення σ^{*2} *незміщеної статистичної оцінки* $\hat{\sigma}^2$ для *параметру* σ^2 *стохастичної структури* моделі.

Для цього виконати наступні розрахунки:

- Підрахувати *теоретичні вартості* моделі $\{k^*_t, t = 1, 2, \dots, n\}$ за формулою:

$$k^*_t = a^*_0 + a^*_1 \cdot q_t + a^*_2 \cdot q_t^2 + a^*_3 \cdot q_t^3, t = 1, 2, \dots, n.$$

- Порахувати *реши* моделі $\{e_t, t = 1, 2, \dots, n\}$ за формулою:

$$e_t = k_t - k^*_t, t = 1, 2, \dots, n,$$

де $\{k_t, t = 1, 2, \dots, n\}$ – *емпіричні вартості* моделі, взяті з числових даних моделі $\{(q_t, k_t), t = 1, 2, \dots, n\}$ за минулий рік.

- *Незміщена статистична оцінка* $\hat{\sigma}^2$ для *параметру* σ^2 *стохастичної структури* моделі визначається формулою:

$$\hat{\sigma}^2 = \frac{1}{n-4} \sum_{i=1}^n e_i^2 = \frac{1}{n-4} \sum_{t=1}^n (k_t - k^*_t)^2.$$

Відповідь: $\sigma^{*2} = 0,0242$

4 Оцінка точності моделі.

Завдання 4. Підрахувати числове значення R^{*2} *множника детермінації* R^2 для збудованої *економетричної моделі*.

Для цього виконати наступні розрахунки:

- Порахувати *середні значення* *емпіричних та теоретичних вартостей* моделі:

$$\bar{k} = \frac{1}{n} \sum_{t=1}^n k_t; \quad \bar{k}^* = \frac{1}{n} \sum_{t=1}^n k_t^*$$

- Порахувати числове значення повної варіації емпіричних та теоретичних *вартостей* моделі:

$$S_K^2 = \sum_{t=1}^n (k_t - \bar{k})^2; \quad S_{K^*}^2 = \sum_{t=1}^n (k_t^* - \bar{k}^*)^2.$$

- Підрахувати числове значення R^{*2} множника детермінації R^2 , який визначається формулою:

$$R^2 = \frac{S_{K^*}^2}{S_K^2} = \frac{\sum_{t=1}^n (k_t^* - \bar{k}^*)^2}{\sum_{t=1}^n (k_t - \bar{k})^2}.$$

Відповідь: $R^{*2} = 0.9861$.

5 Прогнозування на основі нелінійної економетричної моделі.

Завдання 5. Визначити *прогноз* необхідних коштів

$$\{k^{(np)}_1, k^{(np)}_2, k^{(np)}_3\}$$

на перший квартал наступного року, якщо плануються наступні об'єми продукції:

$$\{(q^{(np)}_1 = 5,1), (q^{(np)}_2 = 5,2), (q^{(np)}_3 = 5,4)\}.$$

Розв'язок. Підрахувати *прогнозовані вартості* $\{k^{(np)}_1, k^{(np)}_2, k^{(np)}_3\}$ за формулою:

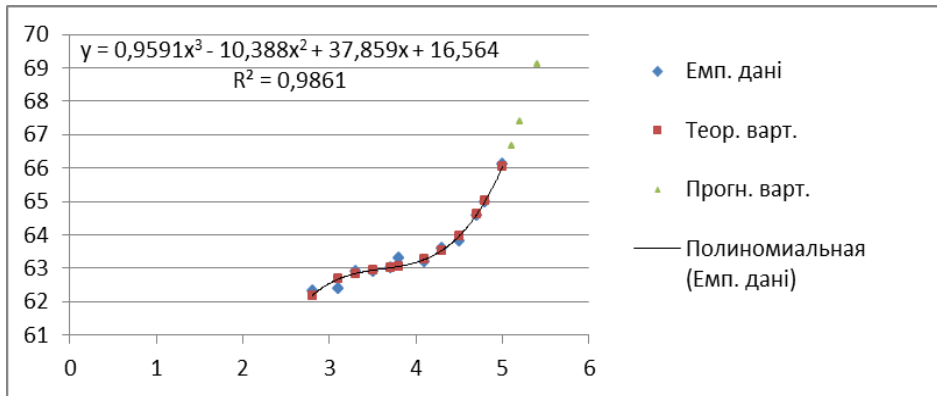
$$k^{(np)}_t = a^*_{0} + a^*_{1} q^{(np)}_t + a^*_{2} (q^{(np)}_t)^2 + a^*_{3} (q^{(np)}_t)^3, \quad t = 1, 2, 3.$$

Відповідь:

$$k^{(np)}_1 = 66,674; \quad k^{(np)}_2 = 67,392; \quad k^{(np)}_3 = 69,107.$$

Завдання 6. Побудувати в аркуші «*Excel*» графік точок, що представляють *числові дані моделі* $\{(q_t, k_t), t = 1, 2, \dots, n\}$, відносно коштів випуску за минулий рік.

- До збудованого графіка додати графік точок $\{(q_t, k_t^*), t = 1, 2, \dots, n\}$, що представляють *теоретичні вартості* моделі.
- Додати графік точок $\{(q_t^{(np)}, k_t^{(np)}), t = 1, 2, 3\}$, що *прогнозовані вартості* на перший квартал наступного року.
- Використовуючи графік точок $\{(q_t, k_t), t = 1, 2, \dots, n\}$ в аркуші «*Excel*», а також опцію «*Формат лінії тренду*», знайти *статистичні оцінки* $\{a^*_{0}, a^*_{1}, a^*_{2}, a^*_{3}\}$ для *структурних параметрів* моделі та числове значення R^{*2} множника детермінації.



3.5. Метод лінеаризації для нелінійної моделі.

1. Метод «лінеаризації моделі». 2. Лінеаризація поліноміальної моделі. 3. Модель для глобальних коштів продукції. 4. Спеціальні функції аркушу «Excel». 5. Параметр стохастичної структури. 6. Прогнозування на основі лінійної економетричної моделі. 7. Аналіз коштів: нелінійна модель.

В прикладі 1 підрозділу 3.4 приведено щомісячні числові дані

$$\{(q_t, k_t), t = 1, 2, \dots, 12\},$$

що представляють глобальну вартість продукції K (в *мл.гр.*) та загальний об'єм продукції Q (в *тис. од.*) протягом року.

Крім того відомі заплановані на перший квартал наступного року об'єми продукції:

$$\{(q^{(np)}_1 = 5,1), (q^{(np)}_2 = 5,2), (q^{(np)}_3 = 5,4)\}.$$

Шляхом проведеного в підрозділі 3.3 безпосереднього аналізу виробничого процесу, було встановлено, що залежність між змінними K та Q добре описує поліном третього степеня:

$$K = a_0 + a_1 \cdot Q + a_2 \cdot Q^2 + a_3 \cdot Q^3.$$

Застосовуючи метод найменших квадратів *безпосередньо до нелінійної моделі* вдалося побудувати «нормальну» систему лінійних рівнянь для знаходження статистичних оцінок структурних параметрів моделі на підставі існуючих емпіричних даних $\{(q_t, k_t), t = 1, 2, \dots, 12\}$. Це, в свою чергу, дозволило побудувати *нелінійну економетричну модель* та побудувати *прогноз* необхідних для цього коштів $\{k^{(np)}_1, k^{(np)}_2, k^{(np)}_3\}$.

Розв'яжемо ту саму задачу, застосовуючи зовсім інший підхід, що широко використовується в практиці економетричних досліджень.

1. Метод «лінеаризації» моделі.

У багатьох випадках, особливо при вивченні явищ на макроекономічному рівні, змінна Y , яка є предметом дослідження, характеризується постійним *приростом* свого значення по відношенню до факторів X_1, X_2, \dots, X_k , що впливають на її формування.

Єдиною *відповідною* функцією, яка може описувати явища подібного типу, є лінійна функція. Отже відповідною *економічно-математичною* моделлю для досліджуваного явища буде лінійна модель:

$$Y = a_0 + a_1 \cdot X_1 + a_2 \cdot X_2 + \dots + a_k \cdot X_k.$$

Ця модель характеризується тим, що вона *лінійна* не тільки по відношенню до незалежних (*пояснювальних*) змінних X_1, X_2, \dots, X_k , а й щодо параметрів a_0, a_1, \dots, a_k .

Остання властивість особливо корисна на етапі *оцінювання параметрів моделі*, оскільки на цьому етапі параметри та незалежні змінні «обмінюються ролями»:

- Параметри виступають, як *незалежні змінні* – їх значення невідомі і потребують свого визначення;
- Тоді як *пояснювальні змінні* X_1, X_2, \dots, X_k , представлені своїми *числовими значеннями*, на підставі яких будується економетрична модель.

Лінійність моделі щодо структурних параметрів a_0, a_1, \dots, a_k суттєво полегшує застосування основних методів їх оцінювання:

- Щодо *класичного методу найменших квадратів*, то ми мали можливість переконатися в цьому в [підрозділі 1.8](#).

У багатьох випадках *нелінійні* функції F , що описують зв'язки між змінними в економетричній моделі, можна зробити *лінійними* по відношенню до параметрів за допомогою простих перетворень («*трансформацій*»). При цьому не має жодного значення те, яким чином *пояснювальні змінні* X_1, X_2, \dots, X_k , з'являються в перетвореній («*трансформованій*») моделі.

- Запроваджуючи нові змінні та обчислюючи на основі емпіричних даних $[Y/X]$ відповідні значення цих нових змінних, вдається звести задачу оцінки параметрів *нелінійної моделі* до оцінки параметрів *лінійної моделі*, подібної до розглянутої в [підрозділі 1.8](#).

Подібне перетворенням називається ще «*лінійною трансформацією*»:

- Лінійна трансформація полягає у зведенні функцій, нелінійних щодо наявних у них параметрів, за допомогою відповідних перетворень до лінійних.

На практиці «лінійна трансформація» відбувається шляхом відповідної «заміни змінної», або іншими словами, у відповідній «підстановці». Можливість такого перетворення значно підвищує практичну значущість класичного методу найменших квадратів та область його використання. Тому не випадково при класифікації економетричних моделей виділяють три основних типи:

- Лінійні моделі;
- Нелінійні моделі, які шляхом лінійної трансформації можна звести до лінійних;
- Нелінійні моделі, які неможливо «трансформувати» до лінійних.

2. Лінеаризація поліноміальної моделі.

В підрозділі 3.3 було встановлено, наприклад, що поліном третього степеня добре описує залежність вартості продукції від її об'єму. Очевидно, що це не єдине економічне явище, для вивчення якого можна ефективно використати нелінійну функцію цього типу.

Поліном ступеня, вищого за перший ($k > 1$):

$$Y = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_k \cdot X^k,$$

очевидно, є нелінійною функцією відносно незалежної змінної X .

Але, в той же час, поліном є лінійною функцією відносно параметрів $a_0, a_1, a_2, \dots, a_k$.

Тому «лінійна трансформація» поліноміальної моделі є дуже простою. Припустимо, що емпіричним матеріалом для побудови економетричної моделі поліноміальної функції ступеня $k > 1$, є результати n незалежних спостережень:

$$\{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$$

змінних (X, Y) .

При цьому, як завжди:

- Для кожної пари (x_i, y_i) координата y_i – це реалізація змінної Y для відповідного значення змінної X , яке представлено координатою x_i .

Суть трансформації полягає в тому, щоб «замінити» нелінійну функцію $Y = Y(X)$ однієї незалежної змінної X на лінійну функцію багатьох змінних:

$$F = F(\mathbf{X}), \mathbf{X} = (X_1, X_2, \dots, X_k).$$

Для цього вистачить ввести до моделі

$$Y = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \dots + a_k \cdot X^k,$$

нові штучні змінні: $X_0 = 1, X_1 = X, X_2 = X^2, \dots, X_k = X^k$, в результаті чого отримаємо наступну модель лінійної регресії:

$$F(\mathbf{X}) = a_0 + a_1 \cdot X_1 + a_2 \cdot X_2 + \dots + a_k \cdot X_k.$$

Емпіричні дані:

$$[\mathbf{Y}/\mathbf{X}] = \begin{bmatrix} y_1 & x_{11} & \dots & x_{1K} \\ y_2 & x_{21} & \dots & x_{2K} \\ \vdots & \vdots & \vdots & \vdots \\ y_n & x_{n1} & \dots & x_{nK} \end{bmatrix}$$

для оцінювання параметрів моделі лінійної регресії з багатьма змінними:

$$F(\mathbf{X}) = F(X_1, X_2, \dots, X_k)$$

будуються на основі статистичних даних $\{(x_t, y_t), t = 1, 2, \dots, n\}$ наступним чином:

$$x_{ij} = (x_t)^i, t = 1, 2, \dots, n, i = 1, 2, \dots, k.$$

Детальна процедура побудови економетричної моделі лінійної регресії представлена в [підрозділі 1.8](#).

3. Модель для глобальних коштів продукції.

Введемо до моделі

$$K = a_0 + a_1 \cdot Q + a_2 \cdot Q^2 + a_3 \cdot Q^3$$

нові штучні змінні:

$$X_0 = 1, X_1 = Q, X_2 = Q^2, X_3 = Q^3.$$

Нелінійна модель з однією змінною Q для нових змінних (X_0, X_1, X_2, X_3) приймас вигляд:

$$Y = A_0 + A_1 \cdot X_1 + A_2 \cdot X_2 + A_3 \cdot X_3.$$

Отримуємо лінійну модель з багатьма змінними (X_0, X_1, X_2, X_3) :

$$y_t = A_0 + A_1 \cdot x_{t1} + A_2 \cdot x_{t2} + A_3 \cdot x_{t3} + \xi_t, t = 1, 2, \dots, n.$$

Зв'язок між *структурними параметрами* $\{a_0, a_1, a_2, a_3\}$ нелінійної моделі та *структурними параметрами* $\{A_0, A_1, A_2, A_3\}$ лінійної моделі виглядає наступним чином:

$$\{a_0, a_1, a_2, a_3\} = \{A_0, A_1, A_2, A_3\}.$$

Завдання 1. Використовуючи числові дані $\{(q_t, k_t), t = 1, 2, \dots, n\}$, що стосуються коштів випуску певних виробів протягом року, збудувати:

• Матицю $\mathbf{X} = \begin{bmatrix} 1 & x_{11} & x_{12} & x_{13} \\ 1 & x_{21} & x_{22} & x_{23} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n1} & x_{n2} & x_{n3} \end{bmatrix} = \begin{bmatrix} 1 & q_1 & q_1^2 & q_1^3 \\ 1 & q_2 & q_2^2 & q_2^3 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & q_n & q_n^2 & q_n^3 \end{bmatrix};$

та

• $y(t) = \begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{bmatrix}$ – вектор-стовпчик складений із спостережень глобальних

коштів продукції K .

Відповідь:

$\mathbf{X} =$	1	3,7	13,69	50,653	$y(t) =$	63
	1	3,8	14,44	54,872		63,3
	1	4,1	16,81	68,921		63,2
	1	4,3	18,49	79,507		63,6
	1	3,5	12,25	42,875		62,9
	1	3,3	10,89	35,937		62,9
	1	3,1	9,61	29,791		62,4
	1	2,8	7,84	21,952		62,3
	1	4,5	20,25	91,125		63,8
	1	4,7	22,09	103,823		64,6
	1	4,8	23,04	110,592		65
	1	5	25	125		66,1

Використаємо наступні позначення:

$\mathbf{A}^{(k)} = \begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \end{bmatrix}$; для вектор-стовпчика, що складається із *структурних параметрів* $\{A_0, A_1, A_2, A_3\}$ моделі;

метрів $\{A_0, A_1, A_2, A_3\}$ моделі;

$\xi(t) = \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix}$ вектор-стовпчика, що складається з *випадкових доданків* моделі

для всіх моментів (t) спостереження; то в матричному запису лінійна модель з багатьма змінними приймає вигляд:

$$y(t) = \mathbf{X} \mathbf{A}^{(k)} + \xi(t).$$

Або

$$\begin{bmatrix} k_1 \\ k_2 \\ \vdots \\ k_n \end{bmatrix} = \begin{bmatrix} 1 & x_{11} & x_{12} & x_{13} \\ 1 & x_{21} & x_{22} & x_{23} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n1} & x_{n2} & x_{n3} \end{bmatrix} \times \begin{bmatrix} A_0 \\ A_1 \\ A_2 \\ A_3 \end{bmatrix} + \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix}.$$

Оцінки Методу Найменших Квадратів

Згідно з методом найменших квадратів вектор $A^{*(k)} = \begin{bmatrix} A^*_{0} \\ A^*_{1} \\ A^*_{2} \\ A^*_{3} \end{bmatrix}$ оцінок стру-

ктурних параметрів $\{A_0, A_1, A_2, A_3\}$ моделі обчислюємо за формулою:

$$A^{*(k)} = (\mathbf{X}^T \cdot \mathbf{X})^{-1} \cdot \mathbf{X}^T \cdot \mathbf{y}_{(t)}.$$

Теоретичні значення моделі

Теоретичні, або *модельні* значення $\{y^*_t, t = 1, 2, \dots, n\}$ змінної Y визначаються формулою:

$$y^*_t = A^*_0 + A^*_1 \cdot x_{t1} + A^*_2 \cdot x_{t2} + A^*_3 \cdot x_{t3}, t = 1, 2, \dots, n.$$

Або в матричному вигляді:

$$\mathbf{y}^*_{(t)} = \mathbf{X} \cdot \mathbf{A}^{*(k)},$$

де вектор-стовпчик $\mathbf{y}^*_{(t)}$ складений з модельних значень $\{y^*_t, t = 1, 2, \dots, n\}$ змінної Y .

Завдання 2. Використовуючи збудовану в завданні 1 матрицю \mathbf{X} та вектор $\mathbf{y}_{(t)}$, визначити числові значення $\{A^*_0, A^*_1, A^*_2, A^*_3\}$ оцінок лінійної моделі з багатьма змінними:

$$A^{*(k)} = (\mathbf{X}^T \cdot \mathbf{X})^{-1} \cdot \mathbf{X}^T \cdot \mathbf{y}_{(t)}.$$

Обчислення виконати у матричній формі.

Відповідь:

$$A^*_0 = 16,564; A^*_1 = 37,859; A^*_2 = -10,388; A^*_3 = 0,9591.$$

Завдання 3. Використовуючи результат завдання 2 підрахувати теоретичні значення $\{y^*_t, t = 1, 2, \dots, n\}$ лінійної моделі з багатьма змінними.

$$\mathbf{y}^*_{(t)} = \mathbf{X} \cdot \mathbf{A}^{*(k)}.$$

Обчислення виконати у матричній формі.

Відповідь:

$$y^*_1 = 63,009; y^*_2 = 63,05; y^*_3 = 63,262; y^*_4 = 63,535; y^*_5 = 62,936; y^*_6 = 62,838; y^*_7 = 62,668; y^*_8 = 62,179; y^*_9 = 63,966; y^*_{10} = 64,603; y^*_{11} = 65,012; y^*_{12} = 65,042.$$

4. Спеціальні функції аркушу «Excel».

Функція «ЛІНІЙН»: побудова моделі.

Завдання 4. Використовуючи емпіричні дані $(\mathbf{y}_{(t)}, \mathbf{X})$ лінійної моделі з багатьма змінними і застосовуючи функцію «ЛІНІЙН» аркушу «Excel», знайти:

- Значення $\{A^*_0, A^*_1, A^*_2, A^*_3\}$ оцінок МНК для структурних параметрів лінійної моделі з багатьма змінними.
- Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури лінійної моделі з багатьма змінними.
- Значення R^{*2} множника детермінації лінійної моделі з багатьма змінними.

Функція «ТЕНДЕНЦІЯ» аркушу «Excel».

Завдання 5. Використовуючи функцію «ТЕНДЕНЦІЯ» обчислити *теоретичні вартості* моделі $\{y^*_t, t = 1, 2, \dots, n\}$, (які називають також «історичним прогнозом»).

5. Параметр стохастичної структури.

Незміщена статистична оцінка $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури лінійної моделі з багатьма змінними визначається формулою:

$$\hat{\sigma}^2 = \frac{1}{n-4} \sum_{i=1}^n e_i^2 = \frac{1}{n-4} \sum_{t=1}^n (y_t - y^*_t)^2 .$$

Завдання 6. Знайти числове значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури лінійної моделі з багатьма змінними. Для цього виконати наступні розрахунки:

- Підрахувати *реши* моделі $\{e_t, t = 1, 2, \dots, n\}$ за формулою:

$$e_t = y_t - y^*_t, t = 1, 2, \dots, n.$$

Відповідь:

$$e_1 = -0,0087; e_2 = 0,2501; e_3 = -0,0621; e_4 = 0,0651; e_5 = -0,0359; e_6 = 0,0622; \\ e_7 = -0,2682; e_8 = 0,1208; e_9 = -0,1664; e_{10} = -0,0028; e_{11} = -0,0121; e_{12} = 0,0581; \\ \sigma^{*2} = 0,0242; \sigma^* = 0,1556.$$

6. Прогнозування на основі лінійної економетричної моделі.

Завдання 7(а). Для запланованих об'ємів продукції на перший квартал наступного року:

$$\{(q^{(np)}_1 = 5,1), (q^{(np)}_2 = 5,2), (q^{(np)}_3 = 5,4)\}.$$

визначити *прогнозовані значення* $\{k^{(np)}_t, t = 1, 2, \dots, s\}$ необхідних коштів, екстраполюючи лінійну модель в область прогнозу.

Обчислення виконати у матричній формі.

Розв'язок.

- На основі запланованих об'ємів продукції $\{q^{(np)}_t, t = 1, 2, 3\}$ знайдемо відповідні значення введених нових штучних змінних (X_1, X_2, X_3) :

$$x^{(np)}_{ij} = (q^{(np)}_t)^i, t = 1, 2, 3, i = 1, 2, 3.$$

Відповідь:

$$\mathbf{X}^{(np)} = \begin{bmatrix} 5,1 & 26,01 & 132,651 \\ 5,2 & 27,04 & 140,608 \\ 5,4 & 29,16 & 157,464 \end{bmatrix}.$$

- Прогнозовані вартості $\{y^{(np)}_1, y^{(np)}_2, y^{(np)}_3\}$ підраховуємо за формулою:

$$y^{(np)}_t = A^*_0 + A^*_1 \cdot x^{(np)}_{t1} + A^*_2 \cdot x^{(np)}_{t2} + A^*_3 \cdot x^{(np)}_{t3}, \quad t = 1, 2, 3.$$

Або в матричному вигляді:

$$\mathbf{y}^{(np)}_{(t)} = \mathbf{X}^{(np)} \cdot \mathbf{A}^*_{(k)},$$

де вектор-стовпчик $\mathbf{y}^{(np)}_{(t)}$ складений з *прогнозованих на основі лінійної економетричної моделі значень* необхідних коштів.

Відповідь:

$$y^{(np)}_1 = 66,674; \quad k^{(np)}_2 = 67,392; \quad k^{(np)}_3 = 69,107.$$

Завдання 7(б). Визначити прогнозовані значення

$$\{y^{(np)}_t, \quad t = 1, 2, \dots, s\},$$

використовуючи для цього функцію «*ТЕНДЕНЦІЯ*».**Відповідь:**

$$y^{(np)}_1 = 66,674; \quad k^{(np)}_2 = 67,392; \quad k^{(np)}_3 = 69,107.$$

7. Аналіз коштів: нелінійна модель.

$$K = a_0 + a_1 \cdot Q + a_2 \cdot Q^2 + a_3 \cdot Q^3.$$

K – глобальні кошти продукції; Q – загальний об'єм продукції

Враховуючи проведену лінеаризацію моделі маємо вектор статистичних оцінок структурних параметрів $\{a_0, a_1, a_2, a_3\}$ нелінійної моделі:

$$\{a^*_0, a^*_1, a^*_2, a^*_3\} = \{A^*_0, A^*_1, A^*_2, A^*_3\}$$

де $\{A^*_0, A^*_1, A^*_2, A^*_3\}$ – отримані в завданні 2 значення МНК-оцінок структурних параметрів $\{A_0, A_1, A_2, A_3\}$ лінійної моделі.

Завдання 8. Обчислити теоретичні значення нелінійної моделі:

$$\{k^*_t, \quad t = 1, 2, \dots, 12\}$$

за формулою:

$$k^*_t = a^*_0 + a^*_1 \cdot q_t + a^*_2 \cdot q_t^2 + a^*_3 \cdot q_t^3, \quad t = 1, 2, \dots, 12.$$

Відповідь:

$$k^*_1 = 63,009; \quad k^*_2 = 63,05; \quad k^*_3 = 63,262; \quad k^*_4 = 63,535; \quad k^*_5 = 62,936; \quad k^*_6 = 62,838; \\ k^*_7 = 62,668; \quad k^*_8 = 62,179; \quad k^*_9 = 63,966; \quad k^*_{10} = 64,603; \quad k^*_{11} = 65,012; \quad k^*_{12} = 65,042.$$

Завдання 9. Визначити *прогнозовані значення*

$$\{k^{(np)}_t, \quad t = n + 1, n + 2, \dots, n + s\}$$

необхідних коштів, *екстраполюючи* гелінійну модель в область прогнозу:

$$k^{(np)}_t = a^*_0 + a^*_1 \cdot q^{(np)}_t + a^*_2 \cdot q^{(np)}_t{}^2 + a^*_3 \cdot q^{(np)}_t{}^3, \quad t = 1, 2, \dots, s.$$

Відповідь:

$$k^{(np)}_1 = 66,674; \quad k^{(np)}_2 = 67,392; \quad k^{(np)}_3 = 69,107.$$

3.6. Методи передачі та захисту інформації.

1. Проблеми управління децентралізованими системами. 2. Хешування даних. 3. Процедура «зашифруй та порівняй». 4. Блоки та дані, що в них знаходяться. 5. Структура заголовку блоку: «корінь Меркла».

1. Проблеми управління децентралізованими системами.

З'ясувавши, що технологія блокчейн в своїй основі скерована на створення та практичне використання складних *децентралізованих* систем, ми прийшли до висновку, що адмініструвати ними значно важче, ніж «звичайними», тобто *централізованими*, в яких ця функція покладена на «*центральный сервер*». Фізичне існування децентралізованої системи та *реальне* виконання нею передбачених проектом завдань пов'язане, перш за все, з *переховуванням, перетворенням, передачею, розповсюдженням та обміном інформації*.

Якщо взяти до уваги, що перше своє *реальне* практичне втілення технологія блокчейн знайшла в фінансовій сфері, а продуктом цього втілення були «*цифрові гроші*», то стане зрозумілим, наскільки *важливою* є інформація, що обертається в цій мережі. Тому природно виникають наступні питання:

- Якщо в мережі відсутні будь-які *сервери*, то де ця інформація зберігається?
- Очевидно, що об'єми даних в подібних мережах – величезні. Незрозуміло, яким чином можна організувати *надійний* обмін нею між учасниками мережі?
- Яким чином можна гарантувати її *незмінність*?
- Як *захистити* функціонування мережі від стороннього *втручання*?
- Якщо всі учасники мережі «*рівні*» в своїх правах (тобто ніхто спеціально *не відповідає* за виконання певних *покладених на нього* обов'язків щодо управління системою чи обслуговування її функціонування), то яким чином взагалі здійснюється її *адміністрування*?

Відповідь на ці та багато інших подібних питань проста:

- Технологія блокчейн не виникла на «*порожньому*» місці.
- За своєю суттю вона не містить нічого *принципово нового*, що було б невідоме науці раніше.
- Творці блокчейн-мереж успішно *використали* технологічні досягнення з *інших сфер* науково-технічної діяльності.

В першу чергу до цих «*сфер*» варто зарахувати сучасні розділи прикладної математики та інформатики, об'єднані спільною назвою «*математична кібернетика*». Творчо розвиваючи, «*комбінуючи*» та

«компілюючи» відповідним чином методи цих дисциплін, припускаючись помилок та наполегливо виправляючи їх, конструктори перших успішно працюючих *крипто-мереж* змогли розв'язати *переважну більшість* принципів проблеми, що виникали при їх створенні.

2. Хешування даних.

Однією з базових *вимог*, що забезпечують успішне функціонування мережі блокчейн, є здатність цієї системи ефективно перетворювати наявну в ній інформацію відповідно до потреб тих завдань, які вона покликана розв'язувати.

- Серед головних математичних інструментів, що використовуються для цього, є *хешування даних*.

Хешування – це універсальний засіб *обробки даних*, що застосовується при розв'язуванні практично всіх основних завдань мережі, пов'язаних з зберіганням, охороною, перетворенням та обміном інформації.

Використання цієї процедури пронизує всі аспекти роботи системи блокчейн. Її можна зустріти:

- ✓ При створенні *адресації* в блокчейн-системах;
- ✓ В методах, що дозволяють безпечно *обмінюватись* даними (*контроль* недоторканості та *електронний підпис*);
- ✓ В процедурах «*майнінгу*» блокчейн-мереж, які підтримують деякі крипто валюти, ітп.

Хеш-функції (або «*геш-функції*») широко використовуються в багатьох математичних дисциплінах, зокрема пов'язаних з інформатикою та обробкою даних.

Перш за все *хешування даних* слід розглядати як один з *базових елементів* їх шифрування. Тому, що хеш-функція *не шифрує* дані, а лише створює певний їх «*відбиток*» або «*витиск*» з цих даних. Згідно з визначенням:

- *Хешування* – це метод перетворення за допомогою спеціальних алгоритмів вхідного масиву даних *довільної довжини* у стандартизований бітовий рядок *фіксованої довжини*.

При цьому:

- Функції хешування *не мають ключа* і покликані захистити *цілісність даних*.

Алгоритми хешування побудовані таким чином, щоб виключити ситуації, коли *різні вхідні набори даних* отримують *однаковий результат* перетворення.

- Така подія називається «*колізією*».

3. Процедура «зашифруй та порівняй».

Оскільки об'єм вхідної інформації може бути довільним, а отриманий в результаті роботи алгоритму її хеш має *стандартизований вигляд фіксованої довжини*, то, очевидно, певні «втрати» інформації є неминучими. В тому сенсі, що формально *хеш-функція* – це «одностороння» функція.

- Не існує «оберненого» алгоритму, який би дозволяв однозначно відновити вхідний масив даних маючи в розпорядженні його хеш.

Єдина в певному сенсі «конструктивна» процедура отримання «прообразу» хешу дістала назву:

- «Методу грубої сили»

Вона фактично рівнозначна звичайному *перебору варіантів*, та може бути використаною, якщо маємо певну множину («масив даних»), серед яких є також дійсний «прообраз».

Алгоритмічно процедура дуже проста:

- *Зашифруй та порівняй.*

Використовуючи алгоритм хешування даних, *послідовно* визначаємо хеші для чергових *масивів даних* з заданої множини, сподіваючись кожного разу, що *отриманий хеш (аж раптом!!!)* співпаде з *заданим*.

Запропонувати якийсь обґрунтований чи раціональний спосіб вибору для перевірки чергового масиву з заданої множини *неможливо*.

Варто підкреслити одну з головних властивостей вже існуючих алгоритмів, і одночасно одну з головних вимог при створенні нових способів хешування:

- *Мінімальна зміна вхідних даних неодмінно призводить до кардинальної зміни їх хешу.*

Для ілюстрації (в підручниках) зазвичай, наводиться наступний *яскравий приклад*.

- Перший із хешів має вигляд:

9ffefb933ed06a04b99dd172c8ee73f59ac7fc3d

- Другий:

10406aa1f6c0c1610fa15455abe43c73484dda32

Це результат дії одного з найпростіших алгоритмів хешування SHA-1. Важко знайти щось «спільного» в наведених «*послідовностях символів*». Хіба що їх кількість.

- Прообразом першого хешу є слово:

Decentralization

- Другого:

Decentralisation

які відрізняються лише *однією літерою* z ↔ s.

Створення *унікального «відбитку»*, яким є хеш, для будь-якого масиву даних дає можливість легко та надійно контролювати *недоторканість* інформації під час її передачі у відкритих мережах:

- Вистачить *«прикласти»* до неї цей цифровий *«відбиток»*, використовуючи загальновідомий алгоритм хешування.
 - Перевірка недоторканості даних зведеться до *хешування* отриманого масиву та порівняння отриманого хешу з *«прикладеним»* до нього цифровим *«відбитком»*.

4. Блоки та дані, що в них знаходяться.

Наступний ключовий принцип мережі блокчейн, який навіть закріплений в назві технології – це здатність створювати *блоки даних* та підтримувати між ними *нерозривний зв'язок*.

- Дослівно *«блокчейн»* означає *«ланцюг блоків»* (*«числових контейнерів»*), в яких зберігається найрізноманітніша інформація.

Блоки – це *базові структурні елементи*, що складають систему. Розташовані вони в строгому *хронологічному* порядку, який не можливо змінити:

- Блоки міцно з'єднують спеціальні *криптографічні замки*.

Неможливо також ані *«вставити»* новий блок, або ж *«видалити»* вже існуючий *всередині ланцюга*, чи *внести зміни* до записаної до блоку інформації.

В своєму *«класичному»* варіанті, згідно з визначенням:

- *Блокчейн* – це *однозв'язний список*, в якому кожний *наступний блок* посилається на *попередній*.

В цю систему є можливість тільки *добавляти* інформацію у вигляді *нових блоків в кінці ланцюга*.

Видалення та зміна інформації є неможливою.

Технологічно блок реалізується наступним чином.

- Всі дані, розміщені в ньому, враховуючи їх зміст та характер, можна поділити на дві частини:
 1. *«Технічні»*, або *«службові»*, що стосуються безпосередньо функціонування та адміністрування мережею;
 2. *«Основні»* дані, що стосуються реалізації тих завдань, задля яких мережа була створена (наприклад *список транзакцій* для передачі числових активів між учасниками мережі; *контракти*; *документи* про власність; або просто *записи фактів*).

Тому в структурі блоку можна виділити дві основні частини.

- Перша частина – *заголовок*, що містить *технічні* дані.
- Друга частина – *основні* дані.

До цих даних можна застосувати алгоритми хешування та «*відобразити*» їх у вигляді хешу стандартної довжини.

- Обчислюючи хеш даних *заголовку* ми, тим самим, фіксуємо *стан* всього блоку і *виключаємо* можливість втручання в його цілісність.
- Якщо ж, крім того, елементом заголовку кожного нового блоку буде хеш заголовку попереднього – то обчислюючи хеш заголовку нового блоку ми створимо нерозривне їх з'єднання.

А в наслідку отримаємо нерозривний ланцюг:

- Втручання в будь-який *біт* даних будь-якого блоку всередині ланцюга призведе до перерахунку всіх хешів.

Іншими словами, зважаючи на властивості алгоритмів хешування, можемо констатувати наступне:

- Навіть «*найдрібніша*» зміна існуючих в мережі даних призведе до зміни «*не до впізнання*» хешу («*відбитку*») всієї мережі.

5. Структура заголовку блоку: «*корінь Меркла*».

Опишемо в загальних рисах більш детально *структуру* заголовку.

Зрозуміло, що кожна конкретне практичне втілення *блокчейн-мережа* може мати *свої особливості*, але деякі *загальні, принципові* для даної технології елементи притаманні *всім без винятку*.

- Заголовок нового блок починається з його *порядкового номеру*.

Якщо мережа функціонує довго і відбувалися *модифікації* програмного забезпечення, то додатково до *порядкового номеру* надається інформація про *номер версії*. При цьому в залежності від *версії структури блоку* та *алгоритми обробки* розміщеної в ньому інформації *можуть змінюватися*.

- Наступна частина заголовку – це *хеш заголовку попереднього*, що забезпечує цілісність даних всього ланцюга.

Виняток становить початковий блок.

Це – «*блок № 1*», або, як ще його називають – «*генезисний блок*». Він відрізняється від всіх наступних тим, не *містить посилання на попередній*.

- Важливим елементом заголовку є *час створення блоку*.

Він записується у вигляді числа, що визначає:

- Кількість секунд, які минули від 1-го січня 1970 р..

Такий формат прийнятий в системі «*Unix*» та в сумісних з нею системах.

- Наступна частина заголовку присвячена безпосередньо «транзакціям», що зберігаються в цьому блоці.

Ця частина заголовку складається з двох чисел:

1. Кількість «транзакцій» в блоці;
2. «Корінь Меркла».

Корінь Меркла – це сукупний хеш всіх «транзакцій» що знаходяться в цьому блоці, обчислений згідно з алгоритмом «бінарного дерева», запропонованим в 1979 р. американським криптографом Рудольфом Мерклом.

Значення «кореня Меркла» – це «відбиток» в заголовку блоку «основної» інформації, яка стосується даних «ділової» частини блоку.

Оскільки хеш заголовку цього блоку буде *частиною* заголовку наступного за ним блоку – то «корінь Меркла» виконує роль *додаткової гарантії* недоторканності даних щодо виконаних раніше операцій.

3.7. Транзакції в системах блокчейн та принцип «балансу».

1. Платіжні блокчейн-мережі.
2. Системи типу «банк-клієнт».
3. «Рахунок» клієнта в блокчейн-системі.
4. Транзакція в блокчейн-системі.
5. «Баланс» активів клієнта та «баланс» в блокчейн-мережі.
6. Комісійні виплати в блокчейн-системі.

1. Платіжні блокчейн-мережі.

Описуючи в загальних рисах структуру інформації, що розміщена в блоках мережі, ми умовно поділили її на дві основні частини. Вигляд та зміст однієї з них, а саме *заголовку*, були коротко представлені.

Розглянемо тепер, як можуть формуватися та виглядати дані, що стосуються реалізації основних завдань системи блокчейн. Оскільки спектр сфер можливого застосування технології блокчейн дуже широкий і в останні роки ми спостерігаємо нові приклади успішного її втілення щоразу в нових галузях, то відповідно і зміст цієї інформації може бути різним.

Тому зупинимось на структурі даних «ділової» частини блоку, що відповідає *платіжним блокчейн-мережам*.

Перший вдалий приклад практичної реалізації технології блокчейн, що успішно функціонує і сьогодні – це мережа *блокчейн Біткоїн*. В даному випадку цей приклад є найбільш доречним, адже йдеться про *основні принципи* формування інформації, «відбитком» якої є «*корінь Меркла*» в заголовку блоку.

Від самого початку проект *Біткоїн* створювався як звичайна *децентралізована платіжна мережа*, досить «*примітивна*» за своїми можливостями, якщо порівнювати її навіть з подібними сучаснішими блокчейн-системами.

- Тому в мережі *блокчейн Біткоїн* поняття «*транзакції*» (висловлюючись образно) було реалізоване «в чистому вигляді», без будь-яких «надбудов» та «додатків».

Це дає можливість сконцентруватися на суті питань, що нас цікавлять.

2. Системи типу «банк-клієнт».

Децентралізовані платіжні *блокчейн*-мережі кардинально відрізняються від існуючих он-лайн систем типу «*банк-клієнт*» (назвемо їх «звичайними»).

- Головна ознака «звичайної» систем – наявність *центрального органу* (банку або іншої фінансової установи).

Для того, щоб стати учасником такої системи, необхідно мати в ній свій *рахунок*.

- Рахунок клієнту відкриває *центральный орган* та видає йому реквізити доступу до *інтернет-банку*.

Всі рахунки та дані про клієнтів *централізовано* зберігаються та охороняються від несанкціонованого доступу на серверах фінансової установи.

- Для отримання доступу до можливості реалізації будь-якої операції («*транзакції*») треба спочатку пройти «*вхідний контроль*».

Якщо з якихось причин *центральный сервер не працює*, то доступ до власних активів *неможливий*.

Якщо ж система працездатна, а клієнт успішно пройшов *вхідний контроль*, то він може *здійснити* заплановану операцію, знову ж таки, *повідомивши* всі її деталі *центральному органу*.

- Практичною реалізацією *транзакції* (наприклад – *переведення* фінансових коштів з рахунку на рахунок) проводить посередник (у вигляді *фінансової установи*), стягуючи при цьому *комісію*, розмір якої він же і встановлює.

3. «Рахунок» клієнта в блокчейн-системі.

В *блокчейн*-системах нічого такого немає, оскільки взагалі відсутній *посередник*, тобто *центральный орган*. Іншими словами – немає ані *центрального серверу*, ані *рахунків*.

- Учасником *блокчейн-системи* може стати кожен бажаючий, хто має доступ до Інтернету.

Програмне забезпечення будь-якої платіжної *блокчейн-системи* знаходиться у відкритому доступі. Його можна «*скачати*» на свій комп'ютер та простим натиском відповідної клавіші в інте-

рфейсі «програми-клієнта» створити свій власний «рахунок» в системі:

- Таким «рахунком» буде автоматично створена самою системою «адреса користувача».

Адреса утворюється відповідно до закладених в даній блокчейн-мережі алгоритмів на основі жорстко пов'язаних між собою двох ключів:

➤ *Секретного.*

Секретний ключ може (наприклад) генеруватися випадковим чином.

➤ *Відкритого.*

Відкритий – обчислюється на підставі секретного за допомогою, знову ж таки, прийнятих в даній системі алгоритмів асиметричної криптографії.

«Адреса» – це фактично модифікація відкритого ключа з використанням декількох процедур хешування та спеціального символічного кодування.

Таким чином, з одного боку:

- З'являється зручна для «візуального» сприйняття адреса.

А з іншого боку:

- Ця адреса надійно захищена від будь-яких спроб її «зламання».

Це єдині, загальні «гарантії безпеки», які система пропонує своїм учасникам.

Оскільки посередник в системі блокчейн відсутній, то після генерації адреси за свою власну безпеку в проведенні операцій та зберіганні «активів» відповідає безпосередньо сам клієнт:

- Якщо учасник мережі загубить секретний ключ, то автоматично втратить доступ до всіх активів, що пов'язані із адресою, яка генерувалася на його основі.
- Всі необхідні ключі та адреси, включаючи і секретний, зберігаються на його комп'ютері.
- На цьому ж комп'ютері клієнт виконує всі дії, передбачені відповідною операцією («транзакцією»).

4. Транзакція в блокчейн-системі.

Для того, щоб зрозуміти специфіку проведення операцій в децентралізованих системах, використаємо застосований вже прийом та порівняємо «звичайну» і «блокчейн» системи.

Візьмемо для прикладу переказ коштів. Нагадаємо, як відбувається ця операція в «звичайній» типовій системі «банк-клієнт».

Банк, в якому знаходиться рахунок «платника», виконує наступні дії:

- Встановлює «вартість» послуги (комісію).
- Перевіряє стан рахунку платника на наявність необхідних коштів.
- Віднімає суму переказу та суму комісії від коштів на рахунку «платника».
- Суму переказу додає до коштів на рахунку «отримувача».
- Суму «комісії» залишає собі в якості оплати за послугу.

В блокчейн-системі все відбувається цілком інакше:

- «Посередник» там взагалі відсутній;

Натомість

- «Рахунків» (як таких) взагалі не існує.

Тому немає можливості ані «від чогось відняти суму переказу», ані «до чогось її додати».

В блокчейн-мережі кожна транзакція – це набір посилань двох типів:

- Перший тип:

- Посилання на колишні надходження на адресу «платника»,
Ці посилання називаються в блокчейн-мережі «входами» на адресу «платника».

- Другий тип:

- Посилання на адреси «отримувачів» коштів, яким вони будуть переводитись.
Ці посилання в блокчейн-мережі називаються «виходами» з адреси «платника».

Тому:

- Якщо один з учасників мережі хоче перевести іншим учасникам певні «кошти», то спочатку мусить довести, що він ці «кошти» має.

Звідси посилання першого типу – на «входи», тобто колишні надходження:

- Множина цих посилань має бути такою, щоб «набрати» необхідну для переказу суму.

Посилання другого типу, тобто «виходи», це адреси одного або кількох отримувачів цих коштів.

- Очевидно, що «вихід» на адресі платника одночасно є «входом» на адресі отримувача, який він зможе використовувати у своїх майбутніх розрахунках.

В мережі існує та строго витримується наступне правило «балансу»:

- Сума всіх активів на «виходах» повинна дорівнювати сумі всіх активів на «входах».

Якщо сума всіх «входів» конкретної транзакції *перевищує* суму всіх «входів» на адреси інших учасників, то «платник» з метою збереження «балансу» в мережі формує додатковий «вхід» на свою власну адресу в розмірі цього надлишку.

Тобто «*решта*» від операції утворює окремий «вхід» на адресу платника.

5. «Баланс» активів клієнта та «баланс» в блокчейн-мережі.

В більшості існуючих децентралізованих платіжних блокчейн-мережах для формування транзакцій та ведення балансу застосовується система UTXO: (*Unspent Transaction Output – невитрачені входи транзакцій*).

Кожен учасник блокчейн мережі має копію всіх проведених в ній операцій, починаючи від першого (генезисного) блоку.

Тому:

- Кожен учасник може перевірити «стан рахунку» будь-якого іншого учасника, обчислюючи суму всіх «входів» та «виходів» на його адресу.

Залишок не потрачених «виходів» і є «рахунком» клієнта мережі блокчейн, тобто «балансом» його «активів».

Відповідальність за успішне проведення операції, тобто за те, що переведені кошти потраплять до відповідного учасника, лежить на «платнику».

- Формуючи «виходи» транзакції платник передбачає, що кожна зазначена там адреса має свого власника в мережі.

Якщо якась з адрес буде введена з помилкою, то транзакція, яка на неї посилается, буде, однак, системою прийнята, але переказані там кошти будуть *втраченими і виключеними з обігу* в системі.

- Що стосується адреси «входів» «платника», то система захищена від *шахрайства*, тобто його можливих спроб послатися на «виходи», які йому не належать.

Обов'язковими елементами будь-якого посилання на «вхід» є *відкритий ключ та електронний підпис* платника.

- Використовуючи закладені в системі алгоритми, проводиться перевірка *легітимності* посилань на входи;
- В разі виявлення помилки – транзакція просто ігнорується та не включається до блоку тим вузлом, що формує його до мережі.

6. Комісійні виплати в блокчейн-системі.

Кожна операція мережі блокчейн має свій унікальний номер, що *не може повторюватись*. Його генерують, як правило, використовуючи *хеш* самої операції.

А це, як відомо, означає:

- Ймовірність *колізій* (в даному випадку – *повторення* номеру операції) практично *нульова*.

Для підтримки *недоторканості* даних та захисту від *несанкціонованого* втручання використовується наступний прийом:

- В *«тілі транзакції»* розміщується *хеш попередньої операції* того блоку, в якому вона знаходиться.

Подібно, як і в ситуації з заголовком – це додатковий елемент захисту інформації.

Як вже підкреслювалось:

- *Відкриті ключі* та *електронні підписи* власників всіх *«входів»* операції теж присутні в додатковій службовій інформації, що супроводжує кожну транзакцію.

Переважна більшість блокчейн-мереж з метою мотивації *«вузлів»* (тобто учасників системи), які створюють блоки, передбачає за це винагороду (*«комісію»*). Таким чином існує два типи винагороди для учасників системи:

- Перша (*«основна премія»*) – це винагорода за створення блоку.

Розмір основної премії є заздалегідь відомим та фіксованим.

- Друга (*«комісія»*) – це додаткова винагорода за *створення конкретної транзакції*.

Кожен *«творець»* може самостійно встановити розмір своєї *«комісії»*.

Однак величина *«комісії»* регулюється самою мережею:

- Розмір комісії впливає на *пріоритетність* транзакції, а отже на *час очікування* в черзі, аж буде включена до чергового блоку.

Безпосередньо розмір комісійних виплат в *«тілі транзакції»* відсутній. Подібно, як і *«стан рахунку»*, величину *«комісії»* можна встановити опосередковано:

«Решта» (тобто окремий *«вхід»* на адресу платника) буде меншою на цю суму від *фактичної* різниці між *«входами»* та *«виходами»* даної операції.

3.8. Роль криптографії та шифрування в блокчейн технології.

1. Типи шифрування. 2. Симетричне шифрування. 3. Асиметричне шифрування. 4. Алгоритми асиметричного шифрування. 5. Крипто-стійкість алгоритмів шифрування. 6. Алгоритми дискретного логарифмування.

Наступний «стовп», що тримає потужну «будівлю» блокчейн-ідустрії, яка стрімко зростає, утворює математична дисципліна під назвою «Криптографія»:

- Надійні та стійкі до «зламання» криптографічні алгоритми гарантують безпеку та недоторканість блокчейн-мережа.

Якщо розглядати умовний «теоретичний фундамент» технології блокчейн, що складається з *n* 'яти розділів сучасної математики та інформатики, то криптографія є його «ядром», або «несучим елементом».

- Можна з цілковитою впевненістю стверджувати, що без криптографії технології блокчейн просто б не існувало.

1. Типи шифрування.

Шифрування є визначальним чинником, що пронизує всі інші елементи розподіленого реєстру, яким є блокчейн-мережа, цементує і утримує весь проект.

- Завдяки використанню методів сучасної криптографії, в блокчейн-мережах забезпечується цілісність та недоторканість інформації під час проведення операцій.
- Криптографія гарантує також безпечне зберігання та обмін даних.

Все це дозволяє ефективно охороняти активи користувачів мережі та захищати їх право власності.

Згідно з визначенням:

- Шифрування – це оборотне перетворення даних, з метою приховання інформації.

Таке перетворення виконується у «по-символьній» формі згідно з відповідними алгоритмами, а результатом є отримання шифрованого тексту.

- Алгоритм перетворення називається ключем шифрування.

Маючи ключ легко відновити початкові дані, тобто розшифрувати їх.

- Подібне перетворення вважається санкціонованим.

У випадку відсутності ключа можна спробувати отримати інформацію з зашифрованого тексту несанкціонованим шляхом.

- Процес несанкціонованого відновлення початкових даних називається дешифруванням;
- Створення ключа дешифрування називається зламанням шифру.

З погляду на характер методів, що використовуються при перетворенні даних, виділяють два основних типи шифрування:

- *Симетрична* криптографія.
- *Асиметрична* криптографія.

2. Симетричне шифрування.

➤ У випадку симетричного шифрування один і той самий ключ використовується як для *шифрування*, так і для *розшифрування*.

Найбільш відомою реалізацією цього типу методів криптографії була створена на початку минулого століття в Німеччині шифрувальна машина «Енігма». Її шифри в ті часи вважалися «незламними».

За кілька років до початку другої світової війни польській розвідці вдалося отримати деякі коди та принципи побудови машини і завдяки цьому відтворити машину та спробувати розібратися в алгоритмах шифрування. Всі напруження по «Енігмі» вдалося вчасно (перед окупацією Польщі) передати британській розвідці.

- Створена там потужна група математиків-криптологів, що отримала назву «команда Тьюрінга», успішно зламала «ключ Енігми».

Серед фахівців в питаннях дешифрування, був в цій групі також Алан Тьюрінг, один з творців математичної кібернетики. Її ж дослідження щонайменше на рік прискорили закінчення другої світової війни.

- Багато дослідників вважають цей період початком розвитку сучасної криптографії.

Великі практичні потреби і не тільки в військовій сфері, але й в багатьох інших галузях господарства, сприяли швидкому розвитку методів криптографії та перетворення її окрему математичну дисципліну.

Одночасно з удосконаленням методів шифрування удосконалювались також методи дешифрування.

- Так, наприклад, шифр «Енігми», який в 30-х роках вважалися «незламними», в 60-х був вже криптографічно-слабким.

З появою комп'ютерів зламання навіть найскладніших симетричних алгоритмів, що використовувались в той час, перестало бути серйозною проблемою.

Підсумовуючи ж, можемо стверджувати, що:

➤ Симетричні алгоритми шифрування не являються крипто-стійкими.

3. Асиметричне шифрування.

- Новий розділ в розвитку криптографії датується 1976 р. та пов'язується з появою і вдосконаленням виключно крипто-стійких алгоритмів.

Першим серед них вважається алгоритм «Діффі-Хеллмана», описаний в статті Уїтфілда Діффі та Мартина Хеллмана: «Нові напрямки в сучасній криптографії», опублікованій в 1976 р.

Алгоритм цього методу передбачає наявність пари ключів:

- Секретний (закритий) ключ;
- Відкритий (публічний) ключ, який певним чином (за допомогою математичних засобів) пов'язаний з секретним.
 - Теоретично секретний ключ можна відновити, знаючи відкритий.
 - Але практично процес його відновлення представляє собою неімовірно складну математичну задачу.

Це дало змогу обмінюватись секретним ключем використовуючи для цього звичайні канали зв'язку, а саме:

- Необхідно обмінятися відкритими ключами.
- Додати до цього деяку допоміжну розрахункову інформацію.
- Використовуючи цю допоміжну інформацію та спираючись на математичні формули легко відновити у приймаючої сторони спільний секретний ключ.

На практиці шифрування з парою ключів відбувається наступним чином:

- Вибирається певний алгоритм асиметричного шифрування.
- Кожен споживач генерує свій секретний ключ.
- Із отриманого секретного ключа, виконуючи розрахунки за відповідними для вибраного алгоритму математичними формулами, споживач отримує другий ключ, що називається «відкритим» або «публічним».

Публічний ключ не тільки «можна», але й «необхідно» відкрити. Оскільки кожен, хто захоче написати його власнику повідомлення, буде змушений шифрувати інформацію з допомогою цього відкритого ключа. Але, на відміну від симетричної криптографії, метод базується на тому, що:

- Шифрується інформація відкритим ключем;
- А розшифрувати її можна – тільки і виключно – відповідним йому секретним ключем.

Іншими словами відпадає необхідність кожного разу ризикувати та поширювати секретний ключ незахищеними каналами зв'язку

4. Алгоритми асиметричного шифрування.

Нині існує та використовується на практиці величезна кількість алгоритмів асиметричного шифрування різної складності.

- Історично першим вважається алгоритм «Діффі-Хеллмана».

Цей алгоритм відкривав новий етап в розвитку криптографії, але, очевидно, не міг бути ідеальним та вичерпним.

Однією із його суттєвих вад було те, що він, зокрема:

- Не давав можливості підтвердити кожній із контактуючих сторін своєї «особовості», тобто – «автентичності сторін».

Вже через рік, в 1977 р. такий алгоритм шифрування був розроблений. Заснований він був на принципі наявності двох ключів, які користувач створює самостійно, і крім цього був придатний до підтвердження автентичності сторін.

Його авторами-розробниками були американські криптографи Рональд Рівеста, Аді Шамір та Леонард Адлеман. Тому назву «алгоритм RSA» він отримав в вигляді аббревіатури за прізвищами своїх творців.

Варто спеціально відзначити ще одну його властивість:

- Алгоритм RSA започаткував нову групу алгоритмів асиметричної криптографії – алгоритмів факторизаційного типу.

Відновлення секретного ключа в алгоритмі RSA зводилось до задачі факторизації великих чисел, тобто:

- Розкладу натурального числа на добуток його простих множників.

«Математична структура» алгоритму RSA є на дивовиж простою:

- Закритий ключ – це два дуже великих простих числа;
- Відкритий ключ – добуток цих чисел.

Криптографічні властивості алгоритму обумовлені наступною обставиною:

- Якщо множення двох чисел є досить легкою задачею;
- То обернена до неї – розклад отриманого добутку на початкові множники – це завдання виняткової обчислювальної складності.

Задача факторизації чисел, які мають десятки розрядів, не є тривіальною навіть для сучасних комп'ютерів.

- Не створено поки що ефективних алгоритмів її розв'язку, які б суттєво відрізнялися від звичайного «перебору»;
- Або були кращими від методу Ферма, запропонованого ним ще в 1643 р.

5. Крипто-стійкість алгоритмів шифрування.

Поява будь-якого алгоритму шифрування супроводжується атакою на нього, тобто спробою його несанкціонованого зламання. Мотивація цього може бути різна – від злочинної до науково-дослідницької, але результат завжди той самий:

- Рано чи пізно *кожен* криптографічний алгоритм буде *зламано*.

Так сталося і з алгоритмом RSA:

- Вже в середині 2000-го року з'явилася інформація про зламання спочатку 512-бітного, а потім і 1024-бітного ключів RSA.

Очевидно, що з подібною задачею самостійно не зможе справитись жоден комп'ютер (мова про «традиційний» комп'ютер, оскільки з'явилася нова загроза – «квантові» обчислення).

Для атак на алгоритми шифрування створюються певні обчислювальні «кластери», які в розумному часовому проміжку виконують *дешифрування, ламаючи шифр та створюючи в несанкціонований спосіб ключ дешифрування*.

Змагання між *складністю* криптографічного алгоритму та обчислювальною *потужністю* комп'ютерів постійно триває.

- Згідно з *законом Мура продуктивність* комп'ютерних процесорів *подвоюється* кожні 18 місяців.

Тому для збереження *крипто-стійкості* алгоритму RSA необхідно постійно *збільшувати довжину відкритого ключа*, що, очевидно, неможливо.

6. Алгоритми дискретного логарифмування.

Узагальненням алгоритму RSA став алгоритм цифрового підпису DSA, побудований на моделі *дискретного логарифмування*.

Дискретне логарифмування – це одна із задач *модульної арифметики*. Формулюється вона наступним чином:

- Нехай a , b та c – відомі натуральні числа.

- Необхідно знайти значення степені x , в яку необхідно піднести число a , щоб при діленні результату такого піднесення на число b отримати в залишку число c .

Іншими словами:

- Треба знайти натуральне число x , яке б задовольняло умову:

$$a^x \bmod b = c.$$

Наприклад, якщо $5^x \bmod 11 = 4$, то $x = 3$.

Якщо показник степеня (x) буде змінюватись, то буде змінюватись і залишок від ділення на 11:

- Так для $x = 2$ цей залишок дорівнює 3:

$$5^2 \bmod 11 = 3.$$

Але завжди ці залишки будуть належати до множини:

$$5^x \bmod 11 \in \{0, 1, 2, \dots, 10\}.$$

Ця множина має назву «*кільця залишків*» (*кільця відрахувань*).

- У випадку *дуже великих значень чисел a , b , c* , знаходження невідомої величини x є *дуже і дуже складною обчислювальною задачею*.

Саме ця обставина і складає основу алгоритму DSA.

3.9. Автентичність та консенсус в технології блокчейн.

1. Проблема встановлення автентичності сторін. 2. Формування цифрового електронного підпису. 3. Перевірка цифрового електронного підпису. 4. Колективний консенсус в технології блокчейн. 5. «Проблема візантійських генералів». 6. *Стійкість до «візантійських збоїв» в блокчейн-пректах*. 7. *Розв'язок задачі «візантійських генералів»*. 8. *Алгоритми Paxos та Tendermint*.

1. Проблема встановлення автентичності сторін.

Цифровий електронний підпис (або коротко – ЕЦП) є одним з найважливіших елементів технології блокчейн. Проблема перевірки *справжності* даних належить до головних завдань, що необхідно розв'язувати при створенні *децентралізованих розподілених систем* (чи *реєстрів*), якими, зокрема, є блокчейн-мережі.

- ЕЦП безпосередньо пов'язаний з шифруванням даних і покликаний захистити їх від *підробки*, чи *фальсифікації*. Тобто *несанкціонованого відтворення* цих даних зі змінами на користь зловмисника.

Особливо загострилась проблема *автентичності* інформації з появою сучасних комп'ютерних цифрових технологій:

- Підробити чи *сфальсифікувати* незахищену *цифрову інформацію* значно легше, ніж *рукописну*.

Розвиток методів *асиметричної* криптографії дав змогу створити надійний захист *цифрової інформації* від несанкціонованого втручання, *«скріпивши»* її цифровим електронним підписом.

З формальної точки зору цифровий електронний підпис (ЕЦП) – це результат роботи певного *криптографічного* алгоритму на вхід якого подається два необхідних елементи:

- *Хеш* набору даних, які необхідно *«підписати»*;
- *Секретний ключ* власника підпису.

Аналізуючи властивості алгоритмів хешування ми відзначали:

- *Мінімальна* зміна (навіть одного біту) вхідних даних, змінить не до пізнання їх хеш.
 - Сформувати ЕЦП може тільки власник *секретного ключа* і ніхто інший;
 - А підписаний *конкретним підписом* документ вже не може бути змінений в жодному своєму біті.

Можна спробувати використовуючи відкритий ключ відновити обчислювальним шляхом секретний ключ. Але це практично неможливо – тому ЕЦП гарантує *надійний захист* та *недоторканість* зашифрованих даних.

2. Формування цифрового електронного підпису.

Формування цифрового електронного підпису відбувається за наступною схемою:

- Перш за все необхідно обрати *криптостійкий алгоритм асиметричного шифрування*.
- Сформувати на підставі цього алгоритму пару ключів: *секретний та відкритий*.
- Вибрати відповідну до даних, що потребують електронного підпису, *хеш-функцію* (тобто обрати потрібний *алгоритм хешування даних*).
- Обчислити *хеш* блоку даних, що будуть підписуватись.
- Обрати алгоритм формування цифрового електронного підпису.
- Маючи *хеш* набору даних, які необхідно «*підписати*», та *секретний ключ*, запускаємо алгоритм формування підпису.
- Відбувається шифрування *хешу* та набору даних з *секретним ключем* користувача.

Результатом роботи цього алгоритму буде ЕЦП (*сертифікат*), що має вигляд рядка даних.

- Цей підпис додається до початкових даних. Таким чином отримуємо дані, *підписані* цифровим електронним підписом, та передаємо їх по каналах зв'язку.

3. Перевірка цифрового електронного підпису.

З погляду на форму математичної реалізації, для різних алгоритмів формування цифрового електронного підпису його перевірка може відрізнятися.

Але по своїй суті ці способи подібні між собою і відбувається за наступною схемою.

- Загальний принцип такої перевірки передбачає *підрахунок двох результатів*, отриманих *різними* способами.

При цьому при обчисленні одного з них *обов'язково* використовується *відкритий* ключ підписанта. Отримані результати порівнюються і в разі, якщо вони не співпадають, робимо висновок:

- або підпис *підроблений*,
- або ж дані *сфальсифіковані*.

Проілюструємо процедуру перевірки на прикладі алгоритму RSA.

- Перше число, це *хеш* отриманих даних, обчислений за допомогою *хеш-функції*, вибраної на етапі формування електронного підпису.
- Друге число, це *хеш* даних, що передавались, отриманий з електронного підпису, яким *підписані* отримані дані.

Цей *хеш* обчислюється шляхом *дешифрування електронного підпису* з використанням *відкритого* ключа підписанта.

- Якщо отримані дані *автентичні*, то результати цих двох обчислень повинні *співпадати*.
- Якщо ж вони не співпадають, то відбулось порушення недоторканості даних.

4. Колективний консенсус в технології блокчейн.

➤ Останнім, *п'ятим «стовпом»* технології блокчейн є «*Теорія ігор*».

Без цього *теоретичного* розділу сучасної математичної кібернетики, подібно, як і без попередніх чотирьох, практична реалізація функціонуючих на принципах блокчейн-технології систем була б неможливою

Управління будь-якою системою – це процес прийняття та реалізації необхідних в конкретній ситуації рішень.

- В *централізованих системах* до цього покликана одна з головних окремих її *підсистем*.

Умовно її можна назвати «*центром прийняття управлінських рішень*». Він спеціально створюється, щоб *приймати рішення* та слідкувати за їх виконанням всіма іншими підсистемами.

➤ Інноваційний характер та оригінальність *технології блокчейну* саме і полягає у відсутності окремої *управлінської* структури.

Суть поняття: «*розподіл довіри*» та «*колективний консенсус*» визначає *існуючий захист* від фальсифікації та несанкціонованого втручання.

В *децентралізованих системах* кожний «*вузол*» володіє актуальною копією всієї наявної інформації, а алгоритми прийняття остаточних рішень ґрунтуються на *строغو-математично доведених* твердженнях.

- Тому немає сумніву в їх *легітимності*.

Проблеми «*довіри*» та «*консенсус*» виникають при створенні нових «*блоків*» та розміщенні в них *відповідної інформації*. А саме:

- У випадку блокчейн-мереж взаємодіють *рівні в своїх правах* суб'єкти, кожен з яких, очевидно, має свій *особистий інтерес*;
- Яким чином в такій ситуації, приходиться до рішень, що виключають виникнення *конфліктів*, здатних *зруйнувати* систему в цілому?

«*Теорія ігор*» будь-яку складну систему розглядає з двох точок зору:

➤ Перша – це сукупність елементів, що її утворюють, кожен з яких використовує власну *стратегію* для досягнення своєї мети.

У випадку блокчейн-мереж це її *учасники*, або окремі «*вузли*».

➤ Друга – це *цілісність*, тобто окремий «*суб'єкт*»; що теж має свої «*власні цілі*», а отже мусить будувати *стратегії* їх реалізації.

У випадку блокчейн-мереж – мережа в *цілому*.

В теорії ігор відомі приклади, коли *раціональна* з погляду кожного окремого суб'єкта поведінка призводила до *нераціональних* з погляду системи в цілому наслідків.

- Це відбувається у випадку, коли деякі з «*гравців*» намагаються максимізувати власний інтерес коштом збитків системи в цілому.

У випадку *платіжних блокчейн-мереж* це можна наглядно проілюструвати наступним прикладом:

- Якщо хтось із учасників вдався до «*шахрайства*» і йому вдалося «*не добросовісно*» шляхом привласнити активи інших учасників, то «*переможців*» в цій ситуації не буде – прогають *всі*.
- Довіра до мережі буде підірвана і вона припинить своє існування.

Так що «*особисто ефективні*» (на перший погляд) дії зловмисника перетворюються в «*суспільно марні*», і як наслідок – *марні* та *шкідливі* для самого цього зловмисника.

5. «Проблема візантійських генералів».

Неодноразово підкреслювалось, що технологія блокчейн не виникла на «*порожньому*» місці і по суті не містить нічого *принципово нового*, що було б невідоме науці раніше.

- Перший цьому приклад – *хешування даних*, без чого *успішне* функціонування мережі блокчейн в принципі *неможливе*.

В 70-тих роках минулого століття, задовго до появи працюючих мереж, які побудовані на принципах технології блокчейн, активно досліджувалось *хешування даних*. Саме результати цих досліджень були фундаментом створення перших блокчейн-мереж.

- Наступним яскравим прикладом можуть бути проблеми «*розподілу довіри*» та «*колективного консенсусу*».

По своїй суті «*технологія блокчейну*» – це просто нова, більш сучасна версія формулювання відомої в теорії зв'язку проблеми забезпечення безвідмовності засобів передачі інформації та *цілісності* трансферу даних в ненадійному середовищі. Дослідження проводились спільно з військовими Сполучених Штатів при створенні стійкої до відмов замкнутої мережі ARPA (Advanced Research Projects Agency – агентство департаменту Міністерства оборони США).

Коротко цю проблему можна сформулювати наступним чином:

- Чи можна взагалі *сприймати інформацію*, джерело якої або канал зв'язку, яким її отримано, *не викликають цілковитої довіри*?
- А якщо так, то *в якій мірі* слід на неї *покладатися*?

Перше глибоке опрацювання вона знайшла в 1982 р. в статті: «*Проблема візантійських генералів*»// ACM Transactions on Programming Languages and Systems. 1982 р. Т. 4. N3.

Після цього «проблема передачі інформації в ненадійному середовищі» отримала назву «задача візантійських генералів».

Її позначають аббревіатурою BFT, від англійської назви:

- *Byzantine Fault Tolerance* (Синоніми – *Byzantine agreement problem*, *Byzantine generals problem*, *Byzantine failure*).

В технічній мові з'явився навіть спеціальний термін «стійкість до візантійських збоїв» що означає:

- Здатність системи продовжувати функціонувати в скороченому об'ємі, не виходячи повністю з ладу у випадку, коли частина її компонентів працює невірно.

6. «Ненадійне середовище» в «проблемі генералів».

Реальна «суть» задачі в спрощеному формулюванні виглядає так:

- ✓ *n* окремих військових підрозділів, кожен з яких очолює окремий генерал, проводять спільну операцію.
- ✓ Кожен з цих генералів з певною ймовірністю може бути «зрадником» і не виконати наказ, який він отримав від командування.
- ✓ Наказ може мати одну з двох версій:

«наступати» або «відступати»

- ✓ Головна умова успішності операції – *злагодженість* дій.

1. *Найкращий* (серед можливих) наслідок операції:

- *Всі* генерали отримують наказ *«наступати»* і *всі* його виконують.

Тоді спільними зусиллями операція буде *успішно виконана*.

2. *Проміжний* наслідок операції:

- *Всі* генерали отримують наказ *«відступити»* і *всі* його виконують.

Тоді операція не буде *виконана*, але *злагодженість* дій дозволить зберегти війська.

3. *Найгірший* (серед можливих) наслідок операції:

- *Не всі* генерали виконують *той* наказ, який вони отримали.

Тоді частина підрозділів піде в *наступ*, частина розпочне *відступати*, а наслідком *незлагоженості* дій генералів операція не буде *виконана* і війська будуть знищені ворогом.

Виникає питання:

- *Яким чином досягти злагодженості дій генералів в такій ситуації, та уникнути найгіршого серед можливих наслідків операції?*

Тобто:

- *Яким чином досягти консенсусу, що відповідає наказу командування?*

6. *Стойкість до «візантійських збоїв» в блокчейн-пректах.*

В контексті *децентралізованих систем*, побудованих на принципах технології блокчейну, ця задача визначає методи досягнення *«колективного консенсусу»* в процесі управління системою.

- Кожен вузол блокчейн-мережі повинен *чітко виконувати* всі вимоги та *правила*, передбачені та прописані у вигляді його програмних алгоритмів.

При цьому система має відкритий характер, тобто кожен вузол володіє програмним забезпеченням блокчейн-проекту, і (при бажанні) може втрутитись в нього, намагаючись «*модифікувати*» на свою користь.

Тому *стійкість* до «*візантійських збоїв*» в блокчейн-пректах – це перш за все ключовий елемент безпеки при формуванні *колективного консенсусу*.

Система повинна мати здатність протидіяти такого роду «*несанкціонованій атаці*» на неї, якщо навіть таких порушників буде «*багато*».

- Суть *колективного консенсусу*, що застосовується для управління в *децентралізованих системах*, полягає в тому, що мережа сама *відкидає* та *ігнорує* інформацію, що не відповідає загальноприйнятим правилам, якими керується *більшість*.
 - Проблема полягає в тому, щоб для «*розмитой*», нечіткої оцінки – «*багато*» встановити конкретні, чітко окреслені *кількісні межі*.

Тобто необхідно визначити «*критичну масу*» кількості порушників, що може призвести до самознищення системи.

- Відповідь дає розв'язок класичної для теорії ігор «*проблеми візантійських генералів*».

7. Розв'язок задачі «візантійських генералів».

Повернемося до «*умовної*» групи з n генералів, частина серед яких – «*зрадники*», що можуть порушити дисципліну та не виконати наказ від командування.

Розглянемо, яку відповідь на питання: «*Яким чином досягти злагодженості дій генералів в ситуації, що склалася?*» дає теорія ігор.

Єдине припущення, яке було прийняте, звучить так:

- ✓ Кожен з генералів з певною ймовірністю може бути «*зрадником*» і не виконати наказ, який він отримав від командування.

Якщо якийсь конкретний генерал *не є зрадником*, або ж навпаки – знає, що працює в інтересах ворога, то це *єдина певна* інформація, якою він володіє. Тому *єдине*, що йому залишається, щоб прийняти своє рішення, не володіючи ніякими даними щодо інших учасників групи, так це прийняти наступне припущення:

- З ймовірністю $\frac{1}{2}$ кожен з цих генералів може бути *зрадником*.

Очевидно, що цього дуже мало, для того, щоб сподіватися на *сприятливе* (або навіть *проміжне до сприятливого*) спільне рішення.

Єдине розумне рішення в цій ситуації, що дасть можливість надати зміст задачі побудови *оптимальної стратегії колективної поведінки*, це припущення про *прямий обмін* генералами своєю інформацією. А саме:

- ✓ Припустимо, що інформація, якою володіють генерали, це *стандартизований набір даних*.
- ✓ Кожен генерал передає *«свій»* набір даних всім іншим, при цьому зміст всіх $(n - 1)$ наборів даних не обов'язково є той самий.
- ✓ Кожен генерал отримає подібну інформацію від *кожного іншого*, (в сумі $(n - 1)$ наборів даних).

Інформація, що передається, побудована таким чином, що кожен генерал *знає*:

- Що повідомив кожен *конкретний* генерал кожному *іншому конкретному* генералу.

Іншими словами:

- Той об'єм інформації, який отримує кожен учасник групи, дозволяє йому знати не тільки те, *про що* інші поінформували *його* в своїх (адресованих йому *особисто*) повідомленнях генерали.
- Але контролювати всю комунікаційну картину в форматі:
 - «Хто, що і кому повідомив».

Таким чином є можливість:

- По-перше – *знайти* та проаналізувати *розбіжності* в різних повідомленнях.
- По-друге – на підставі цього аналізу виявити *«нелояльних»* генералів та оцінити їх *долю* в загальній масі.

Математично доведено наступний результат:

- Якщо кількість *«лояльних»* вузлів *перевищує* $2/3$, то система буде *стійкою* до «візантійських збоїв».
В цьому випадку *консенсус* буде досягнутий.
- Якщо кількість *«лояльних»* вузлів *менша від* $2/3$, то система втрачає свою працездатність.
В цьому випадку децентралізована система *стає некерованою*.

7. Алгоритми Paxos та Tendermint.

Проблема *«розподілу довіри»* та *«колективного консенсусу»* виникла в 2008 – 2009 роках при створенні реально діючих (до наших днів) розподілених *децентралізованих* платіжних систем.

Алгоритми ж та термінологія математичних задач з області теорії ігор, які об'єднує назва «проблема візантійських генералів», розроблялися 30-40 років раніше.

Як вже говорилося – дослідження фінансувалися Міністерством оборони США та стосувалися проблеми забезпечення *безвідмовності* засобів передачі інформації та *цілісності* переданих даних в *ненадійному середовищі*.

Творці технології *блокчейн* успішно скористалися цими розробками та вже готовими, перевіреними і надійно працюючими алгоритми. Більше того, згадана «проблема забезпечення безвідмовності засобів передачі інформації» має свій «аналог» та відповідні розв'язання у вигляді конкретних програмних продуктів в області інформатики.

➤ Якщо термінологію «проблеми візантійських генералів» «перекласти» на мову інформатики, то вона є абстрактним представленням класу програм, призначених до *активізації* ряду пристроїв системи, таких, як:

- Процесори в комп'ютері;
- Комп'ютери в мережі;
- Роботизовані заводські виробничі лінії;
- Вузли в ланцюгу розподілених мереж (з блоками, чи без них), тощо.

В контексті *блокчейн-мереж* – це «управління роботою учасників мережі».

Таким чином в області розподілених обчислень (зокрема в *блокчейн-мережах*) успішно використовуються такі сімейства протоколів, як, наприклад, *Raxos* або *Tendermint*, що дозволяють знаходити *консенсус* в мережі з ненадійними вузлами, ліквідуючи тим самим загрозу її відмови в результаті непередбачуваних збоїв.

- *Raxos* (Паксос) – це алгоритм, що досягає *консенсусу* в розподілених системах, передаючи повідомлення в два етапи комунікації.
- *Tendermint* – ще один алгоритм *консенсусу*, стійкий до «візантійських збоїв».

Це, фактично, *модифіковані* версії відомих алгоритмів, що враховують *особливості блокчейн-мереж*, а саме:

- Той факт, що це *однорангові* мережі.
- Спосіб *формування* блоків в *блокчейн-мережах*.
- Групування розміщеної а них *інформації*.
- Особливості зв'язків блоків в ланцюгу.
- Криптографічну перевірку їх *автентичності*, тощо.

3.10. Аналітичні методи виділення тренду в часових рядах.

Економетрико-статистичні методи в дослідженні економічних процесів.

1. Національний дохід (National Income, *NI*). 2. Статистичні показники динаміки національного доходу. 3. Вибір аналітичної форми моделі тенденції розвитку. 4. Економетрична модель тенденції розвитку змінної V_t .

Підставою для дослідження фінансового ринку є часові ряди $\{y_1, y_2, \dots, y_n\}$, що представляють фактичні значення явища, яке вивчається. Серед аналітичних методів дослідження варто виділити метод визначення тренду на підставі цих спостережень. Він полягає на побудові причинно-наслідкової моделі *тенденції розвитку*, (див. підрозділ 2.15) яка вказує головний напрямок розвитку цього явища.

Суть його в тому, щоб видалити з часового ряду *випадкову складову*, тобто похибку, що з'являється внаслідок впливу випадкових чинників під час спостережень.

➤ Ця складова називається ще *випадковими коливаннями*, а побудова лінії тренду – *згладжуванням* часового ряду.

Лінія тренду $f(t)$, $t = 1, 2, \dots, n$, або *економетрична* модель часового ряду, будується на підставі його фактичних значень:

$$\{y_1, y_2, y_3, \dots, y_n\} = \{y_t, t = 1, 2, \dots, n\},$$

тобто даних, отриманих шляхом статистичних спостережень.

Роль незалежної змінної (тобто «*причини*») в цій моделі відіграє час: $t = 1, 2, \dots, n$, а відповідна процедура виглядає наступним чином:

- Приймається конкретний *гіпотетичний* математичний вигляд моделі, тобто визначається функція $f(t)$, $t = 1, 2, \dots, n$, яка встановлює залежність згладжених (*фактичних*) значень елементів часового ряду досліджуваного явища від часу, без впливу на нього випадкових чинників.
- За допомогою методів математичної статистики оцінюються необхідні параметри моделі з подальшою статистичною верифікацією отриманих результатів.

1. Національний дохід (National Income, *NI*).

Проілюструємо реалізацію цієї процедури на конкретному прикладі одного з найважливіших макроекономічних показників – *національного доходу* (англ. *National Income, NI*) (див. підрозділ 2.12). Згідно з визначенням, це:

➤ *Сукупність усіх доходів в економіці домашніх господарств не залежно від того, де вони використовують ресурси, у своїй країні чи за її межами.*

Характеризуючи фінансові відносини (див. підрозділ 1.4) та перераховуючи учасників цих відносин, ми підкресливали, що існує лише один *об'єкт* (або *предмет*) цих відносин:

- Предметом фінансових відносин є *національне багатство*.

На практиці цю категорію можуть представляти подібні, *споріднені*, а отже тісно пов'язані з нею показники, такі як *національний дохід*, *валовий внутрішній продукт* тощо.

Серед *суб'єктів* фінансових відносин виділимо перш за все такі категорії:

- *Держава* як окремий суб'єкт;
- *Підприємства*;
- *Окремі працівники*.

Тому одна з основних функцій фінансів (а саме *функція розподілу*) полягає у *поділі* внутрішнього валового продукту *між суб'єктами* фінансових відносин. Категорія національного багатства є не лише базовим поняттям економічного життя, а й ключовим поняттям економічної науки.

У макроекономічному аналізі ця категорія відіграє роль *синтетичної міри* загального рівня економічного розвитку аналізованого регіону чи країни.

- Це означає, що неможливо дослідити будь-який аспект чи сферу соціально-економічних явищ, ігноруючи цей показник.

Зважаючи на практично необмежену кількість можливих факторів, що формують цю *синтетичну* змінну, можна очікувати, що для її аналізу можна буде ефективно використати методи *часових рядів*.

- ✓ Особливість цих методів полягає в тому, що вони *не проникають* у суть *взаємних зв'язків* окремих факторів, що впливають на досліджувану змінну, а дозволяють *описати загальну закономірність* розвитку *синтетичного показника*, який нас цікавить, внаслідок цієї взаємодії.

2. Статистичні показники динаміки національного доходу.

При побудові *економетричної* моделі *тенденції розвитку* можна використовувати статистичні методи аналізу *короткотермінових змін* (див. підрозділ 2.10), тобто аналізу динаміки національного доходу в проміжку $t \in \{1, 2, \dots, n\}$.

Нехай $\{V_1, V_2, \dots, V_n\}$ – часовий ряд, що представляє величину національного доходу (V_t) протягом n років поспіль ($t = 1, 2, \dots, n$).

Короткотермінові зміни досліджуються наступним чином:

- ✓ Вибирається *основа для порівняння*, тобто *конкретний* період, що *умовно* вважається як нульовий: $t_0 = 0$.
- ✓ Потім значення V_t національного доходу за аналізований період t порівнюється зі значенням V_0 національного доходу за базовий період.

Основними *мірами* динаміки національного доходу в коротко-строковій перспективі є:

- Абсолютні прирости національного доходу ($\Delta V_{t/0}$) із *фіксованою* основою порівняння (V_0):

$$\Delta V_{t/0} = V_t - V_0, t = 1, 2, \dots, n.$$

- Відносні прирости національного доходу ($\Delta V_{t/0}/V_0$) із *фіксованою* основою порівняння (V_0):

$$\frac{\Delta V_{t/0}}{V_0} = \frac{V_t - V_0}{V_0}, t = 1, 2, \dots, n.$$

- *Ланцюгові* прирости національного доходу ($\Delta V_{t/t-1}$) із змінною основою порівняння ($t_0 = t - 1, V_0 = V_{t-1}$):

$$\Delta V_{t/t-1} = V_t - V_{t-1}, t = 1, 2, \dots, n.$$

- *Темп абсолютного приросту* (T_t) за період t (*темп*) – це *відносний ланцюговий* приріст ($\Delta V_{t/t-1}/V_{t-1}$) зі змінною основою порівняння (V_{t-1}):

$$T_t = \frac{\Delta V_{t/t-1}}{V_{t-1}} = \frac{V_t - V_{t-1}}{V_{t-1}}, t = 1, 2, \dots, n.$$

Вищезазначені показники, що стосуються динаміки національного доходу в минулому, можуть дати багато корисної інформації про *стан економіки, її ефективність* тощо.

Побудована з їх допомогою *економетрична* модель *тенденції розвитку* дозволяє визначити можливі значення цього показника в майбутньому:

- Її можна використовувати для *прогнозування* розміру національного доходу в майбутньому.

3. Вибір аналітичної форми моделі тенденції розвитку.

Нехай V_t означає величину національного доходу в момент часу t . Першим кроком процедури побудови *економетричної* моделі *тенденції розвитку* для цього показника є вибір її *аналітичної форми*, тобто визначення конкретної математичної функції $f(t)$, яка представляє загальну закономірність розвитку національного доходу.

- Основний принцип такого вибору полягає в тому, що функція $f(t)$ повинна «добре відповідати» значенням $\{V_1, V_2, \dots, V_n\}$ часового ряду, які були фактично зареєстровані в результаті спостережень.

Графік точок $\{(1, V_1), (2, V_2), \dots, (n, V_n)\}$ в системі координат tOV та аналіз форми отриманої на графіку «*смуги*» в поєднанні зі знанням динаміки розвитку конкретних математичних функцій можуть бути корисними для цього. Але часто простий візуальний аналіз графіка є недостатнім для однозначного визначення аналітичної форми $f(t)$ моделі.

Для визначення типу функції $f(t)$ можна використовувати згадані вище статистичні показники динаміки національного доходу в проміжку $t \in \{1, 2, \dots, n\}$, тобто міри величини *короткотермінових змін*.

➤ Припустимо, що характерною особливістю часового ряду

$$\{V_1, V_2, \dots, V_n\}$$

для національного доходу за декілька попередніх періодів часу є *постійний темп абсолютного приросту*.

Це означає, що відносні ланцюгові прирости часового ряду $\{V_1, V_2, \dots, V_n\}$ знаходяться на «більш-менш» *постійному рівні* (p). Тобто:

$$\frac{\Delta V_{t/t-1}}{V_{t-1}} \approx p.$$

Вибираючи це припущення за *основу*, визначимо *аналітичну формулу* $f(t)$ моделі тенденції розвитку, яка описує динаміку зміни національного доходу. Часовий ряд V_t , $t = 1, 2, \dots$, можна розглядати як функцію часової змінної t :

$$V_t = V(t), t = 1, 2, \dots,$$

в якій аргумент t приймає натуральні значення.

Вводячи аналогічно до абсолютного приросту $\Delta V_{t/t-1}$, абсолютний приріст Δt змінної t за формулою: $\Delta t = t - (t - 1) = 1$, прийняту умову можна записати наступним чином:

$$\frac{\Delta V_{t/t-1}}{V_{t-1}} \approx p \cdot \Delta t, \text{ або } \frac{\Delta V_{t/t-1}}{\Delta t} \approx p \cdot V_{t-1}.$$

Узагальнимо тепер це припущення та будемо вважати, що воно виконується не лише для одиничних часових інтервалів: $\Delta t = 1$, але й для *часових інтервалів Δt будь-якої довжини*, меншої від одиниці.

Припустимо також, що змінна V_t – неперервна, а спостереження проводяться досить часто. Тоді, враховуючи останнє співвідношення, це припущення можемо записати у наступному вигляді:

$$\frac{dV_t}{dt} \approx p \cdot V_t, \text{ або } \frac{dV_t}{V_t} \approx p \cdot dt.$$

Тобто:

$$\ln(V_t) \approx p \cdot t + C.$$

де C – довільна константа.

Отже, можна зробити висновок, що для *механізму розвитку* показника V_t , який описує значення національного доходу за період t , справедлива наступна рівність:

$$V_t \approx e^{pt+C} = e^C \cdot e^{pt} = b \cdot e^{pt},$$

де символ b , подібно до C , означає довільну додатну константу (в цьому випадку $b = e^C$).

Таким чином:

➤ Прийняте припущення $\frac{\Delta V_{t/t-1}}{V_{t-1}} \approx p$ однозначно визначає аналітичну

форму тренду $f(t)$ моделі тенденції розвитку національного доходу V_t , а саме – тренд буде експоненціальною функцією:

$$f(t) = b \cdot e^{pt}, t > 0.$$

4. Економетрична модель тенденції розвитку змінної V_t .

Отже значення $\{V_1, V_2, \dots, V_n\}$ часового ряду для послідовних моментів часу $t \in \{1, 2, \dots, n\}$, можна записати наступним чином:

$$V_t = f(t) + \xi_t = b \cdot e^{pt} + \xi_t, t = 1, 2, \dots,$$

де символ ξ_t означає значення випадкових коливань у момент часу t .

Позначимо: $a = e^p$. Тоді модель тенденції розвитку для національного доходу V_t приймає форму:

$$V_t = b \cdot a^t + \xi_t, t = 1, 2, \dots,$$

Знайдемо інтерпретацію параметру a .

• Рівність $\Delta V_{t/t-1}/V_{t-1} \approx p$ можна записати наступним чином:

$$p \approx \frac{\Delta V_{t/t-1}}{V_{t-1}} = \frac{V_t - V_{t-1}}{V_{t-1}} = \frac{V_t}{V_{t-1}} - 1.$$

Або

$$\frac{V_t}{V_{t-1}} \approx 1 + p.$$

З іншого боку, рівність $a = e^p$ означає, що при досить малих значеннях параметра p виконується наступна приблизна рівність:

$$a \approx 1 + p.$$

А це означає, що якщо виконується припущення:

$$\frac{\Delta V_{t/t-1}}{V_{t-1}} \approx p,$$

то для величини національного доходу (V_t) і (V_{t-1}) за два послідовні періоди часу ($t - 1$) і t справедливе співвідношення:

$$V_t \approx a \cdot V_{t-1},$$

де

$$a \approx 1 + p.$$

Експоненціальна функція

$$f(t) = b \cdot a^t, t \geq 0,$$

що визначає основний напрямок розвитку національного доходу V_t , містить два невідомі параметри: a і b . Тому наступний крок в процесі побудови *економетричної* моделі тенденції розвитку змінної V_t – це оцінювання невідомих параметрів. Полягає він в тому, щоб:

- Використовуючи відповідні статистичні методи а також наявні значення $\{V_1, V_2, \dots, V_n\}$ часового ряду визначити оцінки $a^* \approx a$; та $b^* \approx b$ невідомих параметрів

3.11. Прогнозування на основі моделі тенденції розвитку.

1. Загальна «схема методу лінійної трансформації». 2. Побудова прогностичної моделі тенденції розвитку. 2. Повернення до нелінійної моделі тенденції розвитку.

1. Загальна «схема методу лінійної трансформації».

Припустимо, що вивчається певне явище, а V означає змінну, яка представляє деякий кількісний його показник. Часовий ряд.

$$V_1, V_2, \dots, V_n,$$

відображає динаміку зміни цього показника для послідовних моментів часу $t = 1, 2, \dots, .$

Необхідно побудувати *точковий* прогноз значень змінної V_t для S наступних моментів часу $t = n + 1, n + 2, \dots, n + S = T$:

$$\{(t, V^{(np)}_t), t = n + 1, n + 2, \dots, n + S = T\}.$$

В [підрозділі 3.5](#) було розглянуто «метод лінійної трансформації» та його практичне застосування в економетричних дослідженнях.

«Лінійна трансформація» відбувається шляхом запровадження до економетричної моделі нових змінних (або іншими словами, у відповідній «підстановці»).

Це дає можливість, обчисливши на основі емпіричних даних $[Y/X]$ відповідні значення нововведених змінних, «трансформувати» нелінійну моделі до лінійної.

Особливо зручно використовувати цей метод у випадку моделі тенденції розвитку, яку вдається звести до лінійної регресії з однією змінною.

До базових показників такої моделі, побудованої методом найменших квадратів, зараховуємо «Множник детермінації R^2 ».

- R^2 – це число, що належить до інтервалу $[0,1]$: $0 \leq R^2 \leq 1$,
- R^2 вимірює «ступінь згідності» теоретичної моделі з емпіричними даними, її відповідності тому, що спостерігаємо в дійсності.
- R^2 дає точну оцінку того, яку частину повної варіації (тобто цілковитої змінності) величини V_t обумовлює «незалежна змінна» t .

Схематично метод лінійної трансформації можна описати наступним чином.

➤ Припустимо, що необхідно знайти функцію

$$f(t), t = 1, 2, \dots, n,$$

яка «найкраще підходить» до емпіричних даних, представлених часовим рядом $\{V_1, V_2, V_3, \dots, V_n\} = \{V_t, t = 1, 2, \dots, n\}$.

1) Формулюємо множину «робочих гіпотез» стосовно аналітичного вигляду функції $f(t)$:

$$\{f_1(t), f_2(t), \dots, f_k(t)\}.$$

2) Для кожної гіпотетичної функції $f_i(t)$, $i = 1, 2, \dots, k$, виконуємо лінійну трансформацію моделі:

$$V_t \rightarrow Z_t.$$

Тобто проводимо перетворення емпіричних даних, що містяться у векторі $\{V_1, V_2, \dots, V_n\}$:

$$\{V_1, V_2, \dots, V_n\} \rightarrow \{Z_1, Z_2, \dots, Z_n\},$$

де

$$\{(t, V_t), t = 1, 2, \dots, n\} \rightarrow \{(u, Z_t), t = 1, 2, \dots, n\},$$

таким чином, щоб звести нелінійну модель $f_i(t)$ до лінійної:

$$z_i(u) = B_i + A_i \cdot u, u = 1, 2, \dots, n.$$

3) Для кожної гіпотетичної функції $f_i(t)$, $i = 1, 2, \dots, k$, будуємо на підставі трансформованих даних:

$$\{(u, Z_t), t = 1, 2, \dots, n\}.$$

лінійну економетричну модель:

$$z^*_i(u) = B^*_i + A^*_i \cdot u, u = 1, 2, \dots, n,$$

де

$$\{B^*_i, A^*_i\}, i = 1, 2, \dots, k,$$

оцінки МНК структурних параметрів

$$\{B_i, A_i\}, i = 1, 2, \dots, k,$$

трансформованої моделі.

4) Для кожної гіпотетичної функції $f_i(t)$, $i = 1, 2, \dots, k$, знаходимо значення

$$R_i^{*2}, i = 1, 2, \dots, k,$$

множника детермінації.

5) Встановлюємо, яка з гіпотетичних моделей $f_i(t)$, $i = 1, 2, \dots, k$, найкраще описує емпіричні дані $\{V_1, V_2, V_3, \dots, V_n\}$.

➤ Такою функцією буде та, для якої значення множника детермінації

$$R_1^{*2}, R_2^{*2}, \dots, R_k^{*2},$$

є найбільшим.

б) Якщо «найкраща» модель $f_i(t)$, встановлена в пункті 5, не є лінійною, то необхідно повернутися до початкової нелінійної моделі $f_i(t)$.

- З цією метою, враховуючи перетворення, що виконувалось при побудові лінійної економетричної моделі:

$$z^*_i(u) = B^*_i + A^*_i \cdot u, u = 1, 2, \dots, n.$$

необхідно застосувати (відповідним чином) обернену до цього перетворення трансформацію. І знаючи оцінки $\{B^*_i, A^*_i\}$ МНК структурних параметрів $\{B_i, A_i\}$ трансформованої моделі, знайти оцінки структурних параметрів нелінійної моделі $f_i(t)$.

2. Побудова прогностичної моделі тенденції розвитку.

Метод лінійної трансформації можна ефективно використати для моделей, що шляхом заміни змінної можна звести до лінійної. До них, зокрема, належать базові елементарні функції:

- 1) лінійна $V_t = b + a \cdot t + \xi_t, t = 1, 2, \dots, ;$
- 2) степенева $V_t = b \cdot t^a + \xi_t, t = 1, 2, \dots, ;$
- 3) експоненціальна $V_t = b \cdot a^t + \xi_t, t = 1, 2, \dots, ;$
- 4) логарифмічна $V_t = b + a \cdot \ln(t) + \xi_t, t = 1, 2, \dots, .$

Приведемо конкретний вигляд відповідних перетворень для кожної з цих функцій.

Лінійна трансформація.

2) У випадку степенєвої моделі:

$$V_t = b \cdot t^a, t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = \ln(b); A = a.$

Відповідні емпіричні дані моделі:

$$\{(u_1, Z_1), (u_2, Z_2), \dots, (u_n, Z_n)\} = \{(u_t, Z_t), t = 1, 2, \dots, n\},$$

де

$$u_t = \ln(t), Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

3) У випадку експоненціальної моделі:

$$V_t = b \cdot a^t, t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = \ln(b)$; $A = \ln(a)$.

Відповідні емпіричні дані моделі:

$$\{(u_1, Z_1), (u_2, Z_2), \dots, (u_n, Z_n)\} = \{(u_t, Z_t), t = 1, 2, \dots, n\},$$

де

$$u_t = t, Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

4) У випадку логарифмічної моделі:

$$V_t = b + a \cdot \ln(t), t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = V_t, t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t = b + a \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = b$; $A = a$.

Відповідні емпіричні дані моделі:

$$\{(u_1, Z_1), (u_2, Z_2), \dots, (u_n, Z_n)\} = \{(u_t, Z_t), t = 1, 2, \dots, n\},$$

де

$$u_t = \ln(t), Z_t = V_t, t = 1, 2, \dots, n.$$

3. Повернення до нелінійної моделі тенденції розвитку.

2) У випадку степеневі моделі:

$$V_t = b \cdot t^a, t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = \ln(b)$; $A = a$.

Якщо $\{B^*, A^*\}$ оцінки МНК структурних параметрів $\{B, A\}$ трансформованої моделі, то оцінки $\{b^*, a^*\}$ структурних параметрів $\{b, a\}$ степеневі моделі обчислюємо за формулами:

$$b^* = \exp(B^*) = e^{B^*}, a^* = A^*.$$

3) У випадку експоненціальної моделі:

$$V_t = b \cdot a^t, t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = \ln(b)$; $A = \ln(a)$.

Якщо $\{B^*, A^*\}$ оцінки МНК структурних параметрів $\{B, A\}$ трансформованої моделі, то оцінки $\{b^*, a^*\}$ структурних параметрів $\{b, a\}$ експоненціальної моделі обчислюємо за формулами:

$$b^* = \exp(B^*) = e^{B^*}, a^* = \exp(A^*) = e^{A^*}.$$

4) У випадку логарифмічної моделі:

$$V_t = b + a \cdot \ln(t), t = 1, 2, \dots,$$

лінійна трансформація моделі має вигляд:

$$Z_t = V_t, t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot u_t = b + a \cdot u_t, t = 1, 2, \dots, n.$$

Параметри: $B = b; A = a$.

Якщо $\{B^*, A^*\}$ оцінки МНК структурних параметрів $\{B, A\}$ трансформованої моделі, то оцінки $\{b^*, a^*\}$ структурних параметрів $\{b, a\}$ логарифмічної моделі обчислюємо за формулами:

$$b^* = B^*, a^* = A^*.$$

3.12. Динаміка національного доходу – лінійна модель.

1. Побудова лінійної прогностичної моделі тенденції розвитку. 2. Лінія регресії моделі: (історичний прогноз). 3. Точковий прогноз в інтервалі емпіричної верифікації. 4. Точність прогнозів *ex-post*.

1. Побудова лінійної прогностичної моделі тенденції розвитку.

(Див. підрозділ 2.1).

Наступний часовий ряд $\{V_1, V_2, \dots, V_T\}$, ($T = 20$) представляє ВВП країни впродовж послідовних 20 років (в млрд. дол. США):

$$\begin{aligned} V_1 &= 416,5; V_2 = 444,2; V_3 = 459,8; V_4 = 473,6; V_5 = 500,2; \\ V_6 &= 540,3; V_7 = 577,2; V_8 = 631,7; V_9 = 694,2; V_{10} = 737,9; \\ V_{11} &= 764,4; V_{12} = 801,7; V_{13} = 859,3; V_{14} = 889,2; V_{15} = 916,1; \\ V_{16} &= 963,2; V_{17} = 1011; V_{18} = 1053,3; V_{19} = 1121; V_{20} = 1212,9; \end{aligned}$$

На підставі цих даних необхідно побудувати прогностичну модель тенденції розвитку

$$V_t = b + a \cdot t + \xi_t, t = 1, 2, \dots, T.$$

Реалізувати поетапно процедуру створення моделі, виконуючи послідовно наступні завдання:

(1). Поділити інтервал спостереження $\{1, 2, \dots, T\}$, а отже і наявні емпіричні дані $\{V_1, V_2, \dots, V_T\}$, на дві частини:

$$\{1, 2, \dots, T\} = \{1, 2, \dots, n\} \cup \{n + 1, n + 2, \dots, n + S\},$$

Інтервал $\{1, 2, \dots, n\}$ трактувати, як область побудови прогностичної моделі; дані з інтервалу $\{n + 1, n + 2, \dots, n + S = T\}$ використати для емпіричної перевірки якості отримуваних прогнозів.

Покласти при цьому:

$$n = 15, S = 5, T = n + S = 20.$$

(2). Побудувати в аркуші «Excel» графік точок $\{(1, V_1), (2, V_2), \dots, (n, V_n)\}$, що представляють *числові дані* $\{(t, V)_t, t = 1, 2, \dots, n\}$ з інтервалу побудови прогностичної моделі.

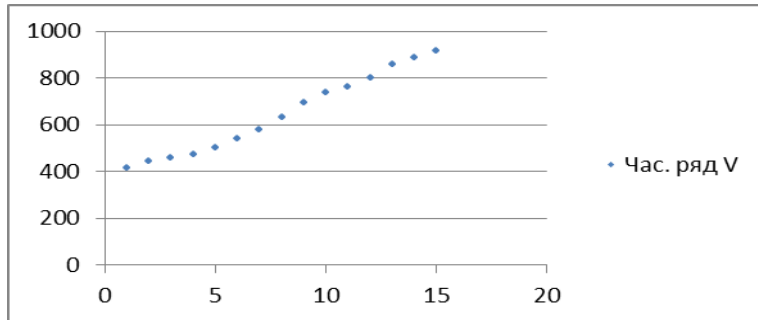


Рис. 1.

Відповідь: Рис. 1.

«Смуга», яку утворюють на графіку точки $\{(1, V_1), (2, V_2), \dots, (n, V_n)\}$, «*несуттєво коливається*» навколо *прямої* лінії. Тому маємо підстави використати для побудови прогнозів *лінійну модель тенденції розвитку*:

$$V_t = b + a \cdot t + \xi_t, t = 1, 2, \dots, n.$$

(3). Використовуючи емпіричні дані моделі $\{(t, V_t), t = 1, 2, \dots, n\}$ та застосовуючи функцію „*ЛІНІЙН*” аркушу «Excel», знайти значення:

$$\{a^*, b^*\} \approx \{a, b\}$$

оцінок МНК для структурних параметрів моделі та числове значення R^{*2} множника детермінації R^2 .

Відповідь: Функція „*ЛІНІЙН*”

a^*	38,507	339,03	b^*
$S^*(a)$	1,3452	12,2307	$S^*(b)$
R^{*2}	0,9844	22,509	σ^*

2. Лінія регресії моделі: (історичний прогноз).

(4). Використовуючи побудовану лінійну модель тенденції розвитку побудувати лінію регресії моделі, тобто обчислити теоретичні значення

$$\{(t, V^*_t), t = 1, 2, \dots, n\}$$

Моделі за формулою:

$$V^*_t = b^* + a^* \cdot t, t = 1, 2, \dots, n.$$

(5). Обчислити теоретичні значення моделі $\{(t, V^*_t), t = 1, 2, \dots, n\}$, (які називають також «*історичним прогнозом*») використовуючи для цього функцію „*ТЕНДЕНЦІЯ*” аркушу «Excel».

Відповідь: $V^*_1 \approx 377,54$; $V^*_2 \approx 416,05$; $V^*_3 \approx 454,55$; $V^*_4 \approx 493,06$; $V^*_5 \approx 531,57$;
 $V^*_6 \approx 570,07$; $V^*_7 \approx 608,58$; $V^*_8 \approx 647,09$; $V^*_9 \approx 685,59$; $V^*_{10} \approx 724,10$;
 $V^*_{11} \approx 762,61$; $V^*_{12} \approx 801,11$; $V^*_{13} \approx 839,62$; $V^*_{14} \approx 878,13$; $V^*_{15} \approx 916,63$.

(6). Додати отримані точки $\{(t, V^*_t), t = 1, 2, \dots, n\}$ до побудованого раніше графіку (Малюнок 1).

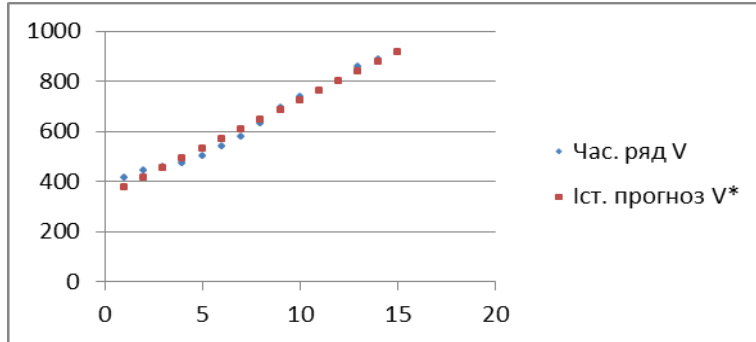


Рис. 2.

Відповідь: Рис. 2..

3. Точковий прогноз в інтервалі емпіричної верифікації.

Значення часового ряду $\{V_{n+1}, V_{n+2}, \dots, V_T\} = \{V_{16}, V_{17}, \dots, V_{20}\}$ для інтервалу $t \in \{n+1, n+2, \dots, n+S\}$ – відомі.

$$V_{16} = 963,2; V_{17} = 1011; V_{18} = 1053,3; V_{19} = 1121; V_{20} = 1212,9;$$

Отже є можливість порівняти їх з прогнозом, що дозволяє зробити побудована модель і тим самим оцінити її «якість».

Тому проміжок $t \in \{n+1, n+2, \dots, n+S\}$ називається інтервалом емпіричної верифікації моделі.

(7). Використовуючи побудовану лінійну модель тенденції розвитку визначити точковий прогноз:

$$\{(s, V^{(пр.)}_{n+s}), s = 1, 2, \dots, S\}, (t = n + s, s = 1, 2, \dots, S), n + S = T.$$

в інтервалі $t \in \{n+1, n+2, \dots, n+S\}$ за формулами:

$$V^{(пр.)}_{n+s} = b^* + a^* \cdot (n + s), s = 1, 2, \dots, S.$$

Відповідь:

$$V^{(пр.)}_{16} \approx 955,14; V^{(пр.)}_{17} \approx 993,65; V^{(пр.)}_{18} \approx 1032,15; V^{(пр.)}_{19} \approx 1070,66; V^{(пр.)}_{20} \approx 1109,17.$$

(8). Визначити прогнозовані значення $\{(s, V^{(пр.)}_{n+s}), s = 1, 2, \dots, S\}$ змінної V_t в інтервалі емпіричної верифікації, використовуючи для цього функції „ТЕНДЕНЦІЯ” аркушу «Excel».

Відповідь:

$$V^{(пр.)}_{16} \approx 955,14; V^{(пр.)}_{17} \approx 993,65; V^{(пр.)}_{18} \approx 1032,15; V^{(пр.)}_{19} \approx 1070,66; V^{(пр.)}_{20} \approx 1109,17.$$

(8). Додати отримані точки:

$$\{(t, V^{(пр.)}_t), t = n + 1, n + 2, \dots, T\}$$

до побудованого раніше графіку (Рис. 2).

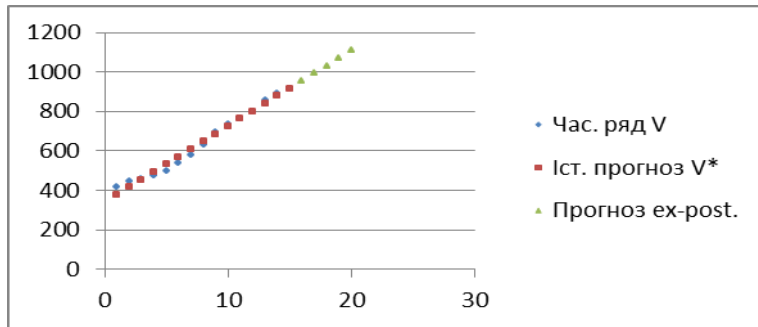


Рис. 3.

Відповідь: Рис. 3.

4. Точність прогнозів ex-post. (Див. підрозділ 2.1).

(10) Використовуючи визначений *точковий* прогноз

$$\{(s, V^{(np.)}_s), s = 1, 2, \dots, S\} = \{V^*_{n+1}, V^*_{n+2}, \dots, V^*_T\}.$$

змінної V_t в інтервалі емпіричної верифікації, а також відомі значення

$$\{V_{n+1}, V_{n+2}, \dots, V_T\}$$

часового ряду обчислити наступні *лінійні* міри точності прогнозів ex-post.

➤ Середню *безумовну* похибку прогнозу ex-post в діапазоні верифікації:

$$ME = \frac{1}{S} \sum_{s=1}^S (V_{n+s} - V^*_{n+s}).$$

Відповідь: $ME = 40,125$.

➤ Середню *відносну* похибку прогнозу ex-post в діапазоні верифікації:

$$MPE = \frac{1}{S} \sum_{s=1}^S \frac{V_{n+s} - V^*_{n+s}}{V_{n+s}} \cdot 100\%.$$

Відповідь: $MPE = 3,52\%$.

➤ Середню *абсолютну* безумовну похибку прогнозу ex-post в діапазоні верифікації:

$$MAE = \frac{1}{S} \sum_{s=1}^S |V_{n+s} - V^*_{n+s}|.$$

Відповідь: $MAE = 40,125$.

➤ Середню *абсолютна* відносну похибка прогнозу ex-post в діапазоні верифікації:

$$MAPE = \frac{1}{S} \sum_{s=1}^S \left| \frac{V_{n+s} - V^*_{n+s}}{V_{n+s}} \right| \cdot 100\%.$$

Відповідь: $MAPE = 3,52\%$.

(11) Обчислити *квадратичні* міри точності прогнозів *ex-post*:

➤ Середньо-квадратичну помилку прогнозу *ex-post*:

$$MSE = \frac{1}{S} \sum_{s=1}^S (V_{n+s} - V^*_{n+s})^2.$$

Відповідь: $MSE = 2821,5$.

➤ Обчислити доданок U^M в складі *квадратичні* міри MSE :

$$U^M = \frac{(\bar{V} - \bar{V}^*)^2}{MSE},$$

де

$$\bar{V} = \frac{1}{S} \sum_{s=1}^S V_{n+s}; \text{ та } \bar{V}^* = \frac{1}{S} \sum_{s=1}^S V^*_{n+s}.$$

Відповідь: $U^M = 0,570$.

➤ Обчислити доданок U^S в складі *квадратичні* міри MSE :

$$U^S = \frac{(\sigma_V - \sigma_{V^*})^2}{MSE};$$

де

$$\sigma_V = \sqrt{\sigma_V^2} \text{ та } \sigma_{V^*} = \sqrt{\sigma_{V^*}^2},$$

а

$$\sigma_V^2 = \frac{1}{S} \sum_{s=1}^S (V_{n+s} - \bar{V})^2; \text{ та } \sigma_{V^*}^2 = \frac{1}{S} \sum_{s=1}^S (V^*_{n+s} - \bar{V}^*)^2.$$

Відповідь: $U^S = 0,383$.

➤ Обчислити доданок U^C в складі *квадратичні* міри MSE :

$$U^C = \frac{2\sigma_V \sigma_{V^*} (1 - r_{VV^*})}{MSE},$$

де

$$r_{VV^*} = \frac{\sum_{s=1}^S (V_{n+s} - \bar{V})(V^*_{n+s} - \bar{V}^*)}{\sqrt{\sum_{s=1}^S (V_{n+s} - \bar{V})^2 \cdot \sum_{s=1}^S (V^*_{n+s} - \bar{V}^*)^2}}.$$

Відповідь: $U^C = 0,047$.

(12) Перевірити справедливість наступних рівностей:

$$MSE = (\bar{V} - \bar{V}^*)^2 + (\sigma_V - \sigma_{V^*})^2 + 2\sigma_V \cdot \sigma_{V^*} \cdot (1 - r_{VV^*}),$$

$$U^M + U^S + U^C = 1.$$

Відповідь:

$$(\bar{V} - \bar{V}^*)^2 = 1610,1; (\sigma_V - \sigma_{V^*})^2 = 1082,8; 2\sigma_V \cdot \sigma_{V^*} \cdot (1 - r_{VV^*}) = 128,6.$$

(13) Використовуючи опцію «Формат лінії тренду» аркушу «Excel», додати до збудованого графіка теоретичну модель а також, знайти статистичні оцінки $\{a^*, b^*\}$ для структурних параметрів моделі і числове значення множника детермінації R^2 .

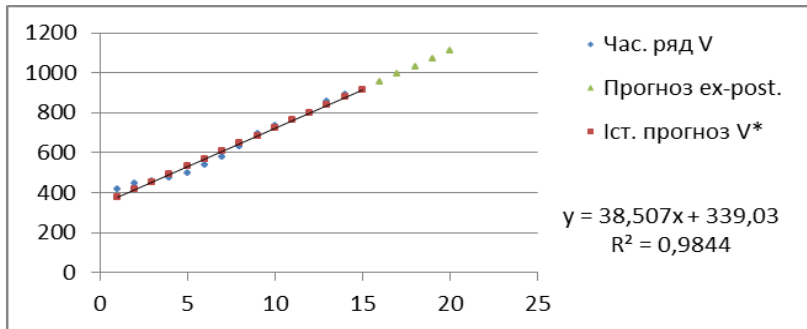


Рис. 4.

Відповідь: Рис. 4.

3.13. Нелінійна модель динаміки національного доходу.

1. Множник детермінації R^2 . 2. Побудова експоненціальної прогностичної моделі. 3. Функція «ЛГРФНАБЛ» аркушу «Excel». 4. Точність прогнозів *ex-post*. 5. Графічна ілюстрація.

1. Множник детермінації R^2 .

В підрозділі 3.10 йшлося, між іншим, про аналітичні методи знаходження функціонального вигляду моделі *тенденції розвитку*, що визначає тренд динаміки макроекономічних показників загального стану економіки певної країни чи регіону, до яких зараховуємо також і ВВП.

При цьому було встановлено, що на практиці досить часто цілком обгрунтованою для змінної V_t буде експоненціальна модель тенденції розвитку:

$$V_t = b \cdot a^t + \xi_t, t = 1, 2, \dots, .$$

Слід відзначити, що наведені в прикладі підрозділу 3.12 емпіричні дані $\{V_1, V_2, \dots, V_T\}$ – це реальні показники, що представляють динаміку розвитку ВВП Польщі в періоді від 1999 р. по 2018 р. Отже маємо можливість перевірити емпіричним шляхом висновки міркувань підрозділу 3.10. Емпіричним показником «якості» моделі (див. підрозділ 3.11) є «Множник детермінації R^2 ».

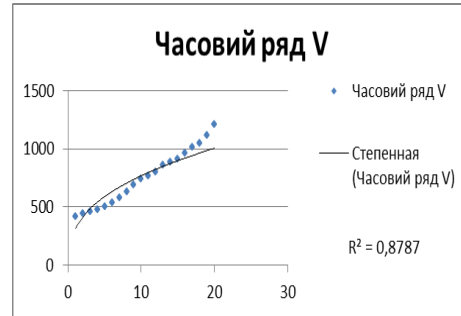
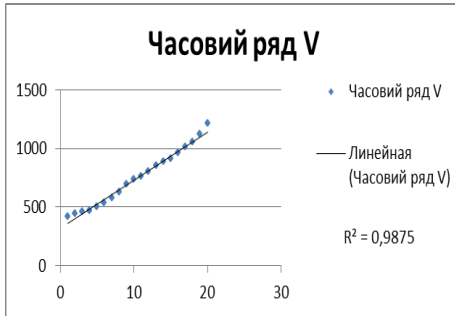
Тому скористаємось опцією «Формат лінії тренду» аркушу «Excel», підраховуючи значення множників детермінації $\{R^2(i), i = 1, 2, 3, 4\}$ для кожної з наступних чотирьох вибраних «робочих гіпотез»: лінійна, степенева, експоненціальна, логарифмічна, та з'ясуємо, яка з них «точніше» описує динаміку цього часового ряду.

(1). Побудувати в аркуші «Excel» графік точок $\{(1, V_1), (2, V_2), \dots, (T, V_T)\}$, що представляють *числові дані* динаміки розвитку ВВП Польщі в періоді від 1999 р. по 2018 р.

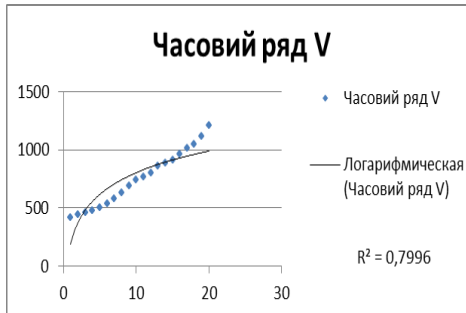
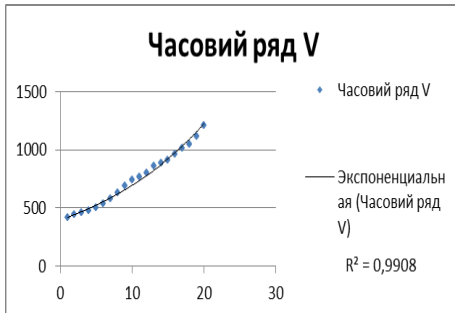
(2). Використовуючи опцію «Формат лінії тренду» аркушу «Excel», додаючи послідовно до збудованого графіка точок $\{(t, V_t), t = 1, 2, \dots, T\}$ часового ряду $\{V_1, V_2, \dots, V_T\}$ наступні теоретичні моделі: «лінійна, степенева, експоненціальна, логарифмічна», знайти для кожної з них числові значення $\{R^2(i), i = 1, 2, 3, 4\}$ множників детермінації:

Відповідь:

1) Лінійна функція: $R^2(1) = 0,9875$; 2) Степенева функція: $R^2(2) = 0,8787$;



3) Експоненціальна $R^2(3) = 0,9908$; 4) Логарифмічна $R^2(4) = 0,7996$.



2. Побудова експоненціальної прогностичної моделі.

Нелінійна (експоненціальна) модель тенденції розвитку.

$$V_t = b \cdot a^t + \xi_t, t = 1, 2, \dots,$$

Або:

$$V_t = b \cdot e^{c \cdot t} + \xi_t, t = 1, 2, \dots, (c = \ln(a)).$$

(3). Лінійна трансформація експоненціальної моделі тенденції розвитку. Провести перетворення емпіричних даних, що містяться у векторі

$$\{V_1, V_2, \dots, V_n\},$$

таким чином, щоб звести нелінійну (експоненціальну) модель до лінійної:

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots, .$$

Розв'язок. Лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, n.$$

Модель

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots, .$$

Параметри:

$$B = \ln(b); A = \ln(a).$$

Відповідні емпіричні дані моделі $\{(t, Z_t), t = 1, 2, \dots, 15\}$:

$$Z_1 = 6,032; Z_2 = 6,096; Z_3 = 6,131; Z_4 = 6,160; Z_5 = 6,215;$$

$$Z_6 = 6,292; Z_7 = 6,358; Z_8 = 6,448; Z_9 = 6,543; Z_{10} = 6,604;$$

$$Z_{11} = 6,639; Z_{12} = 6,687; Z_{13} = 6,756; Z_{14} = 6,790; Z_{15} = 6,820.$$

(4). Застосовуючи класичний метод найменших квадратів до моделі

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots,$$

на підставі перетворених емпіричних даних $\{(t, Z_t), t = 1, 2, \dots, 15\}$, за допомогою функції „**ЛІНІЙН**” аркушу «Excel», знайти:

- Значення $\{B^*, A^*\}$ оцінок МНК для структурних параметрів моделі;
- Числове значення R^{*2} множника детермінації R^2 ;
- Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури моделі.

Відповідь:

A^*	0,0607	5,9526	B^*
$S^*(A)$	0,0018	0,0160	$S^*(B)$
R^{*2}	0,9891	0,0295	σ^*

$$B^* = 5,9526; A^* = 0,048; R^{*2} \approx 0,9891; \sigma^2 \approx \sigma^{*2} \approx 0,00087; \sigma \approx \sigma^* \approx 0,0295.$$

(5). Використовуючи «метод лінійної трансформації» знайти значення оцінок (a^*, b^*) параметрів a і b початкової нелінійної моделі.

Розв'язок. Оцінки (a^*, b^*) параметрів a і b початкової нелінійної моделі обчислюємо на підставі оцінок B^* і A^* параметрів A і B трансформованої моделі за формулами:

$$b^* = \exp(B^*) = e^{B^*}; a^* = \exp(A^*) = e^{A^*}.$$

Відповідь: $a^* = 1,0626; b^* = 384,746.$

(6). **Історичний прогноз.**

Використовуючи побудовану нелінійну модель тенденції розвитку побудувати лінію регресії моделі, тобто обчислити теоретичні значення:

$$\{(t, V_t^*), t = 1, 2, \dots, n\}$$

моделі за формулою:

$$V_t^* = b^* \cdot (a^*)^t, t = 1, 2, \dots, n.$$

Відповідь: $V^*_{1} \approx 408,82$; $V^*_{2} \approx 434,40$; $V^*_{3} \approx 461,58$; $V^*_{4} \approx 490,47$; $V^*_{5} \approx 521,16$;
 $V^*_{6} \approx 553,77$; $V^*_{7} \approx 588,42$; $V^*_{8} \approx 625,24$; $V^*_{9} \approx 664,36$; $V^*_{10} \approx 705,93$;
 $V^*_{11} \approx 750,11$; $V^*_{12} \approx 797,04$; $V^*_{13} \approx 846,92$; $V^*_{14} \approx 899,91$; $V^*_{15} \approx 956,22$.

3. Функція «ЛГРФНАБЛ» аркушу «Excel».

(7). Використовуючи емпіричні дані моделі

$$\{(1, V_1), (2, V_2), \dots, (n, V_n)\},$$

і застосовуючи функцію «ЛГРФНАБЛ» аркушу «Excel», знайти:

- Значення $\{b^*, a^*\}$ оцінок МНК для структурних параметрів моделі;
- Числове значення R^{*2} множника детермінації R^2 ;
- Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури моделі.

Відповідь:

a^*	1,0626	384,75	b^*
$S^*(a)$	0,0018	0,0160	$S^*(b)$
R^{*2}	0,9891	0,0295	σ^*

$$c^* = 0,0607; a^* = 1,0626; b^* = 384,75; R^{*2} \approx 0,9891; \sigma^2 \approx \sigma^{*2} \approx 0,00087.$$

(8). Використовуючи побудовану нелінійну модель тенденції розвитку

$$V_t = b \cdot a^t + \xi_t = b \cdot e^{c \cdot t} + \xi_t, (c = \ln(a)), t = 1, 2, \dots,$$

визначити *точковий* прогноз

$$\{(s, V^{(np.)}_s), s = 1, 2, \dots, S\} = \{V^*_{n+1}, V^*_{n+2}, \dots, V^*_T\}.$$

змінної V_t в інтервалі емпіричної верифікації $t \in \{n + 1, n + 2, \dots, n + S\}$.

Прогнозовані значення $\{V^*_{n+1}, V^*_{n+2}, \dots, V^*_T\}$ обчислити за формулою:

$$V^*_t = b^* \cdot (a^*)^t, t \in \{n + 1, n + 2, \dots, n + S\}.$$

Відповідь: $V^{(np.)}_1 \approx 1016,1$; $V^{(np.)}_2 \approx 1079,6$;
 $V^{(np.)}_3 \approx 1147,2$; $V^{(np.)}_4 \approx 1218,9$; $V^{(np.)}_5 \approx 1295,2$.

4. Точність прогнозів ex-post. (Див. підрозділ 2.1).

(9). Використовуючи визначений *точковий* прогноз

$$\{(s, V^{(np.)}_s), s = 1, 2, \dots, S\} = \{V^*_{n+1}, V^*_{n+2}, \dots, V^*_T\}.$$

змінної V_t в інтервалі емпіричної верифікації, а також відомі значення

$$\{V_{n+1}, V_{n+2}, \dots, V_T\}$$

часового ряду обчислити наступні *лінійні* міри точності прогнозів ex-post.

➤ Середню безумовну похибку прогнозу ex-post в діапазоні верифікації:

Відповідь: $ME = -79,142$.

➤ Середню відносну похибку прогнозу ex-post в діапазоні верифікації:

Відповідь: $MPE = -7,34\%$.

➤ Середню абсолютну безумовну похибку прогнозу *ex-post* в діапазоні верифікації:

Відповідь: $MAE = 79,142$.

➤ Середню абсолютна відносна похибка прогнозу *ex-post* в діапазоні верифікації:

Відповідь: $MAPE = 7,34\%$.

(10). Обчислити квадратичні міри точності прогнозів *ex-post*:

➤ Середньо-квадратичну помилку прогнозу *ex-post*:

Відповідь: $MSE = 6540,2$.

➤ Обчислити доданок U^M в складі квадратичні міри MSE :

Відповідь: $U^M = 0,9577$.

➤ Обчислити доданок U^S в складі квадратичні міри MSE :

Відповідь: $U^S = 0,0198$.

➤ Обчислити доданок U^C в складі квадратичні міри MSE :

Відповідь: $U^C = 0,0225$.

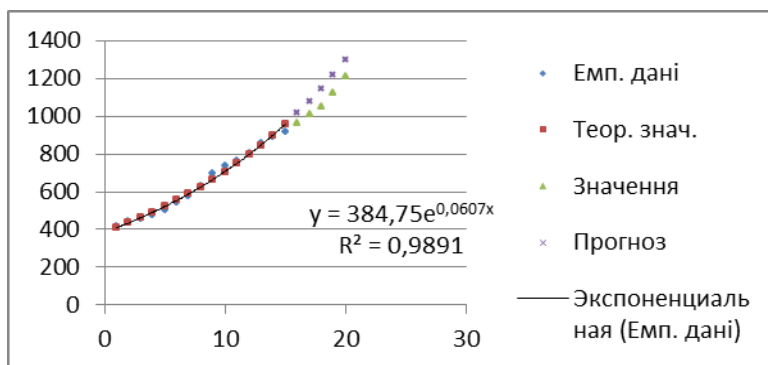
(11). Переконалися в справедливості наступної рівності:

$$U^M + U^S + U^C = 0,9577 + 0,0198 + 0,0225 = 1.$$

5. Графічна ілюстрація.

(12). Побудувати в аркуші «Excel» графік точок що представляють емпіричні дані моделі $\{(t, V_t), t = 1, 2, \dots, n\}$ з інтервалу побудови прогностичної моделі. Послідовно додати до нього графіки наступних точок:

- Історичний прогноз $\{V_t^*, t = 1, 2, \dots, n\}$;
- Застосувати опцію «Формат лінії тренду», «Помістити на діаграму величину достовірності апроксимації R^2 » аркушу «Excel» і знайти статистичні оцінки $\{a^*, b^*\}$ структурних параметрів a і b та числове значення (R^{*2}) множника детермінації R^2 для експоненціальної моделі;
- Відомі значення $\{V_{n+1}, V_{n+2}, \dots, V_T\}$ змінної V_t в інтервалі емпіричної верифікації;
- Точковий прогноз $\{(s, V^{(np.)}_s), s = 1, 2, \dots, S\}$ *ex-post*..



3.14. Передісторія створення мережі «блокчейн-біткойн».

1. Передумови створення цифрових грошей. 2. Перші проекти цифрових грошей: проект «eCash». 3. Проект «В-money». 4. Проект «Bit Gold» та принцип «доведення роботи». 5. Мережа блокчейн біткойн. 3. Алгоритми дискретного логарифмування. 4. Генерування ключів в мережі блокчейн біткойн.

1. Передумови створення цифрових грошей.

В попередніх підрозділах було наведено багато конкретних прикладів, подій та дат, що свідчать про потужні кризові явища на міжнародних фінансових ринках. Аналізуючи їх причини, приходимо до висновку, що часто це є безпосереднім наслідком та яскравим підтвердженням негативних тенденцій в розвитку світової фінансової системи.

Проведемо деякі очевидні паралелі між хронологією згаданих кризових явищ, та хронологією найважливіших подій, що передували практичному втіленню в життя технології *блокчейну*, яку поправу можна назвати *найважливішою новітньою сучасною технологією*.

Вже згадувались ідеї австрійського фінансиста Фрідріха Августа фон Хайєка, представлені ним в далекому 1976 р., коли Інтернету не існувало навіть в творах фантастів, не говорячи про *блокчейн-технології*. Вже тоді були помітними негативні тенденції в розвитку світової фінансової системи. Зрозумілою також була одна із основних причин їх появи:

- Надуживання урядами багатьох держав довіри суспільства в справі грошової емісії, безвідповідальність інституцій, покликаних контролювати та регулювати фінансові установи, неодмінно будуть мати негативні наслідки на всі інші сфери діяльності та призведуть до криз і потрясінь.

Нажаль ситуація постійно ще більше погіршувалась і ці прогнози справдились. В своїй книзі «Приватні гроші» Хайєк наводив аргументи слушності скасування державної монополії в управлінні грошово-фінансовою системою та запровадження конкурентних недержавних фінансових систем.

Ці ідеї зацікавили в першу чергу фахівців в області криптографії та підштовхнули їх до розробки проектів, які безпосередньо стосувалися:

- *Концепцій створення систем децентралізованого, анонімного грошового обігу.*

Комп'ютеризація фінансово-господарських процесів сприяла швидкому розвитку цієї математичної дисципліни, зокрема розробці методів практичної реалізації *цифрового електронного підпису*.

В блокчейн системах, як правило, використовується ЕЦП, побудований на основі методів *асиметричної криптографії*. Головні прин-

ципи формування та перевірки цього ЕЦП вже були представлені в [підрозділі 3.9](#). Але такий підхід, що інколи називають «стандартним» далеко не єдиний, оскільки існує багато інших цікавих рішень (заснованих як на *асиметричній*, так і на *симетричній* криптографії), які успішно розв'язують цю важливу проблему.

2. Перші проекти цифрових грошей: проект «eCash».

Серед великої кількості різноманітних підходів до практичної реалізації електронного підпису варто виділити метод «сліпого підпису». Його називають також «доведенням з нульовим розголошенням» і широко використовують не тільки в платіжних блокчейн-системах, а й, наприклад, в системах електронного голосування.

Технічно метод «сліпого підпису» реалізується наступним чином.

- Певна група учасників системи («вузлів мережі») вибирає собі «довірену особу» (окремий «вузол» мережі до якого всі члени групи мають безумовну довіру).
 - Якщо хтось з групи хоче «скріпити» свою інформацію електронним підписом, він її шифрує та висилає на адресу «довіреного вузла».
 - Не знайомлячись із змістом отриманого «листа» (інформація залишається зашифрованою) довірена особа його підписує своїм ЕЦП.
 - Після цього підписана інформація повертається до відправника.
 - В свою чергу, відправник, отримавши підписану інформацію, розшифровує її, залишаючи при цьому недоторканою ЕЦП довіреної особи.

Саме на основі схеми «сліпого електронного підпису» була створена історично перша система обігу електронних грошей «eCash».

- Її натхненником був американський криптограф Девід Чаум, а концепція системи була викладена в книзі «Сліпі підписи та платежі, які неможливо відстежити», написаній ним в 1982 р.

Сліпий підпис в цьому проекті використовувався для перевірки та авторизації цифрових «банкнот», що знаходились в обігу, а головним завданням «довіреного вузла» (своєрідного банку) був контроль та запобігання від спроб повторного використанню вже витрачених електронних грошей.

- Для технічного та фінансового забезпечення функціонування проекту «eCash» в 1990 р. в Нідерландах була зареєстрована компанія *DigiCash*.
- В 1990 – 1995 рр. вона активно співпрацювала з банківськими платіжними системами (зокрема с системою *VISA*).

Навіть компанія Microsoft співробітничала з *DigiCash* і планувала інтегрувати проект «eCash» в нову (на той час) версію операційної системи Windows 95.

- Однак організаційні прорахунки Девіда Чаума в ведені бізнесу призвели в 1998 р до банкрутства компанії *DigiCash*, її активи були розпродані а проєкт закритий.

3. Проєкт «В-money».

1997 – 1998 р. виявились дуже насиченим на видатні події та потрясіння, що відбулися в світовій сфері фінансів.

- Найбільш помітною серед них була хвиля криз, що зародилася в другій половині 1997 р. на фінансових ринках південно-східної Азії (так званий «*Азіатський грип*») та прокотилася в 1998 р. по всьому світу.

Це вкотре змусило багатьох замислитись над встановлення причин подібних небажаних та загрозливих явищ та необхідністю створення ефективних засобів запобігання їм.

- Очевидним для всіх було те, що джерелом негативних тенденцій в розвитку світової фінансової системи є її *надмірна централізація*.

Державна монополія в фінансовій сфері, її повна залежність від *кон'юнктурних рішень* окремих «персоналій», що виявились на вершині політичної та економічної влади своїх країн, генерувала надмірну «*зарегульованість*» національних економік – *в цілому*, та їх фінансових установ – *зокрема*. Часто причиною потужних світових фінансових криз була *банальна некомпетентність* керівництва фінансових інституцій.

Ідея *децентралізованого грошового обігу* розглядалися багатьма, як одна з можливих відповідей на подібні виклики. Невипадково тому першим реальним діючим втіленням технології *блокчейн* була розподілена *децентралізована* платіжна система. Але створити її вдалося лише через 10 років.

- Натомість перший детальний опис такої системи з'явився саме в 1998 р.

Враховуючи наведені вище обставини, що не дуже сприяли практичній реалізації цього проєкту, він так і залишився в вигляді *рукописної проєктної документації*, однак багато в чому визначив напрямки розвитку технології *блокчейн*, а багато закладених в ньому принципів було використано в першій реально діючій до наших днів платіжній *блокчейн-мережі*.

Проєкт мав назву «В-money» а створив його американський комп'ютерний інженер, випускник Вашингтонського університету *Вей Дай*. Зокрема транзакції з *електронною готівкою* в «В-money» планувалося реалізовувати точно так, як це відбувається в діючих сьогодні *блокчейн-мережах*, а саме:

- *Відкритий* (публічний) *ключ* учасника мережі виконує роль його *адреси* (або номеру *рахунку*).

- Відправник з допомогою свого *секретного ключа* формує цифровий електронний підпис.
- Формує транзакцію, що складається з наявних у нього цифрових активів, закріплює її електронним підписом та переказує на *адресу* отримувача.
- Подібно, як в *блокчейн системах* відправник та отримувач завжди контролюють свої *секретні ключі*, маючи таким чином можливість переказувати один одному електронну готівку.
- Одночасно наявність *секретного ключа* дає їм можливість математично довести право на володіння цими коштами.
 - Таким чином *фактично* перший проект розподіленої *децентралізованої* платіжної системи був створений в 1998 р.

Але цей проект, під назвою «*B-money*», розроблений американським комп'ютерним інженером Вей Даєм, так і залишився в вигляді *рукописної проектної документації*.

4. Проект «*Bit Gold*» та принцип «*доведення роботи*».

В цьому ж 1998 р. був створений наступний проект, який використовував все позитивне з точки зору формування майбутньої технології *блокчейн*, що вже з'явилося в попередніх проектах (зокрема й проекту «*B-money*»).

➤ Була це розподілена *децентралізована* платіжна система «*Bit Gold*».

Її творцем був американський вчений (угорського походження) в галузі криптографії, інформатики та права, *Нік Сабо*.

➤ І хоч проект було розроблено ще в 1998 р., оприлюднений він був лише в 2005 р.

- Принципово новим елементом проекту «*Bit Gold*» в порівнянні з попередніми був присутній в ньому принцип «*доведення роботи*» (*Proof-of-Work*).

Саме на це хотів звернути увагу його автор, використовуючи в назві слово «*золото*». Таким чином він хотів підкреслити, що злиток золота чи зроблена з нього прикраса – це результат *тяжкої, наполегливої* праці багатьох людей різних професій.

Нік Сабо змусив користувачів системи для досягнення своїх цілей (зокрема для емісії *крипто-монет*) розв'язувати складні математичні задачі.

➤ В його проекті необхідно було знайти прообраз *хешу спеціально заданого вигляду*.

А саме:

- Рядок символів, що представляє цей *хеш*, мусить *починатися відрізком*, що складається з *заданої кількості нулів*.

Як відомо, іншого способу, ніж *перебрати* величезну кількість прообразів, щоб (раптом!) *випадково вгадати* потрібний, не існує. З обчислювальної точки зору задача не є складною:

- Співвідношення між розрядністю n (розміром) *хешу*, та кількістю можливих варіантів генерації *хешу*, дорівнює 2^n .

Якщо, наприклад, перші 20 біт хешу повинні бути нулями, то для знаходження правильної відповіді необхідно перебрати *максимально* 2^{20} варіантів, тобто приблизно *біля мільйону*. На це звичайному комп'ютеру необхідно кілька секунд.

➤ Зауважимо, що цей прийом Нік Сабо запозичив у Адама Бека, який подібним чином боровся з розповсюдженням «спаму» у проєкті «*Hash-cash*», створеному в 1997 р.

В цьому проєкті перед тим, як відправити кожного листа, необхідно було отримати *хеш* саме з 20 нулями.

Назва «*Proof-of-Work*» в сучасній криптографії з'явилася пізніше – в 1999 р. Її запровадили криптографи Маркус Якобсон та Ари Джуелс. Конкретний зміст цього виразу в *блокчейн-пректах* наступний:

➤ Знаходження *секретного* прообразу, *хеш* якого задовольняв би по своїй складності певним вимогам.

Його пояснення дуже просте:

- Якщо якийсь з вузлів системи пропонує свою відповідь, то пропускаючи її через процедуру хешування кожен учасник мережі може легко переконатися, чи є вона *правильною*.

Це одночасно буде *однозначним та вичерпним доведенням роботи*, виконаної вузлом для розв'язку цієї задачі.

Принцип «*Proof-of-Work*» незабаром після появи проєкту Ніка Сабо відіграв ключову роль в створенні діючих на практиці *блокчейн-мереж*.

- Поеднавши вже відомі елементи та вводячи нові, Нік Сабо підійшов *дуже близько* до створення функціонуючої мережі цифрових грошей.

Однак ряд нерозв'язаних принципових проблем ще стояли на перешкоді цьому.

➤ Це, зокрема, проблема *інфляції*, що неминуче б виникла при розширенні мережі та зростанні обчислювальних потужностей окремих вузлів.

Тому закладена *фіксована складність* обчислювальної задачі з часом неминуче перестане бути проблемою, а вузли будуть масово «*друкувати*» цифрові гроші.

Залишалися нерозв'язаними ще ряд інших важливих з практичної точки зору проблем:

- Тому проєкт «*BitGold*» *так і не був реалізований*.

3.15. Функціонування мережі блокчейн біткойн.

1. Мережа блокчейн біткойн. 2. Операції над еліптичними кривими. 3. Алгоритми дискретного логарифмування. 4. Генерування ключів в мережі блокчейн біткойн. 5. Формування адреси в мережі блокчейн біткойн. 6. Як потрапити в чергу мережі блокчейн біткойн? 7. «Жива» черга та «медпул».. 8. Майнінг в мережі блокчейн біткойн.

1. Мережа блокчейн біткойн.

Якщо виникає якийсь суспільний запит, то рано чи пізно він знаходить своє практичне втілення. Так сталося й з цифровими грошима – зусилля згаданих «ентузіастів» та сотень тисяч інших представників найрізноманітніших наукових та технічних галузей не були марними.

- 31 жовтня 2008 р. криптографічному товариству була представлена стаття: *Bitcoin BTC: A Peer-toPeer Elektronik Cash System*.

Незабаром викладені в ній ідеї технології блокчейн були втілені в життя у вигляді системи *Біткойн*:

- Це був перший проект, побудований на технології блокчейн.

Автором статті був «таємничий», нікому невідомий *Сатоші Накамото*. Тайна існування Сатоші Накамото є нерозгаданою й донині.

Оскільки принципи побудови систем «*BitGold*» та *Біткойн* дуже схожі, то не виключено, що *Нік Сабо* та *Сатоші Накамото* – це та сама особа, хоч «*претендентів*» на місце Сатоші Накамото дуже і дуже багато.

- В 2007 р. Накамото оголосив, що розпочинає праці над технологією блокчейн біткойн.
- В серпні 2008 р. Сатоші Накамото зарезервував доменне ім'я «*bitcoin.org*».
- В статті, опублікованій в жовтні 2008 р., Сатоші Накамото заявив, що принципові проблеми створення біткойну розв'язані.

В ній було викладено проект створення розподіленої мережі цифрових грошей. В цьому проекті поряд з відомими принципами було описано ряд нових. Це суттєво відрізняло його від вже відомих та виправляли існуючі в них помилки.

Створюючи блокчейн біткойн, Сатоші Накамото склав набір правил (*протокол*), що регламентують роботу мережі.

- Перший (*вихідний*) блок блокчейн біткойну був створений 3 січня 2009 р.

Створив його Сатоші Накамото і в якості нагороди за це отримав 50 біткойнів.

- Це була перша біткойн-готівка, першої реально функціонуючої криптовалюти.

- 12 січня 2009 р. відбулась перша біткойн-транзакція.

В першій *біткойн-транзакції* (яку сам Сатоші Накамото і реалізував) були задіяні 10 біткойнів. Відразу після Накамото в створеній ним мережі з'явився новий її учасник – американський програміст Хел Фінні.

➤ В якості «*тесту*» Сатоші Накамото відправив йому 10 біткойнів.

- Це й була перша в історії реалізована *фізично* транзакція між учасниками мережі.
- Вона була включена до блоку з номером 170.

Спочатку на цю статтю та її практичну реалізацію у вигляді діючої системи, ніхто крім фахівців в області криптографії (подібно до Хела Фінні) не звернув особливої уваги.

Пізніше, коли інформація почала поширюватись, над проектом «*електронних грошей*» багато хто відверто сміявся.

➤ Коли ж вартість однієї монети стала обчислюватись тисячами доларів США (в кінці 2017 р. вартість 1 біткойна сягала майже 20000\$, а в 2021 р. – перетнула межу 60000\$) – вже не було *так смішно*, як на початку.

➤ Наступний «*пік*» – 100000\$ за 1 біткойн досягнув в грудні 2024 р.

Нині кількість подібних *блокчейн-проектів* обчислюється тисячами, а сама «*Біткойн-мережа*» виглядає досить *анахронічно* в порівнянні із багатьма серед них.

- Однак по масштабам капіталізації перша крипто валюта *біткойн* постійно та впевнено очолює список основних цифрових грошей.

2. Операції над еліптичними кривими.

Говорячи про роль криптографії в технології *блокчейн*, зокрема представляючи методи асиметричної криптографії, ми вже описували деякі алгоритми:

- ✓ «*Діффі-Хеллмана*»,
- ✓ Алгоритм *RSA*,
- ✓ Алгоритми *факторизаційного* типу *DSA*, тощо.

Зростання обчислювальних потужностей сучасних комп'ютерів змушує криптографів створювати нові, більш складні алгоритми. Для істотного ускладнення алгоритмів *факторизаційного* типу в 1985 р. були створені «*Алгоритми ECDSA*»:

✓ Алгоритми *ECDSA* – це алгоритми *дискретного логарифмування на основі еліптичних кривих*.

- *Еліптичною кривою* називають множину точок, що задовольняють рівняння:

$$y^2 = x^3 + ax + b.$$

В порівнянні з алгоритмами *DSA*, в яких обчислення відбуваються над *кільцем цілих чисел*, в алгоритмах *ECDSA* обчислення відбуваються над *множиною точок еліптичної кривої*.

Не кожна еліптична крива має необхідні властивості для криптографічного використання – це досить складні речі, які й вивчає криптографія. Ми зупинимось лише на тому, щоб пояснити *принцип побудови* відкритого та закритого ключів.

На множині точок еліптичної кривої можна визначити деякі операції, результатом яких будуть інші точки на цій же кривій. Наведемо приклади таких операцій.

1. Додавання точки самої до себе.

Проведемо *геометричну* ілюстрацію цієї операції.

Очевидно, що наведену процедуру можна описати за допомогою спеціальних формул, спираючись на координати точок, що в ній виступають. Потім, маючи формули, обчислити результат алгебраїчним шляхом за допомогою комп'ютера.

- Нехай $P = P(x, y)$ – точка на еліптичній кривій, що має координати (x, y) . Проведемо до кривої

$$y^2 = x^3 + ax + b.$$

дотичну в точці P .

- Знайдемо тепер координати (x', y') точки $P' = P'(x', y')$, в якій ця дотична перетинає еліптичну криву.

Еліптична крива має дві симетричні відносно осі OX гілки: одну в півплощині $y > 0$, другу – в півплощині $y < 0$.

- Тому проведемо через точку $P'(x', y')$ вертикальну пряму (перпендикулярну до осі OX).
- Знайдемо точку перетину $P''(x'', y'')$ цієї вертикальної прямої з еліптичною кривою на протилежному боці.

Визначення: Точка $P''(x'', y'')$ визначає суму точки P з самою собою:

$$P'' = P + P.$$

2. Множення точки на ціле число n .

Визначення: Суму $(P + P)$ можна назвати також *добутком точки $P = P(x, y)$ на ціле число 2*.

$$P'' = P + P = 2P.$$

Визначення: Якщо починаючи тепер від точки P'' повторити описану процедуру та знайти суму точки P'' з самою собою, то отриманий результат буде називатися *добутком точки $P = P(x, y)$ на ціле число 3*:

$$P''' + P'' = 3P.$$

Будуємо тепер дотичну до точки $3P$, і так далі.

Визначення: Продовжуючи цей процес n разів отримаємо *добуток точки $P = P(x, y)$ на ціле число n* .

$$n \cdot P = (n - 1) \cdot P + (n - 1) \cdot P.$$

3. Алгоритми дискретного логарифмування.

Припустимо тепер, що вибрана відповідна еліптична крива, яка має необхідні властивості для криптографічного використання. Варто зауважити, що консорціум SECG розробив рекомендації щодо вибору параметрів еліптичних кривих:

- «Стандарти для ефективної криптографії».

Ці стандарти використовуються також при реалізації проектів *блокчейн*.

Тоді алгоритм дискретного логарифмування на цій еліптичній кривій будуються дуже просто.

Припустимо, що точки X та P , що належать множині точок цієї еліптичної кривої, задовольняють рівнянню:

$$X = n \cdot P.$$

Припустимо також, що виконані наступні умови:

- Координати точок X та P відомі.
- n – невідоме.

Визначення: Точка X – це *відкритий* (або *публічний*) *ключ*.

Число n – це *закритий* (або *секретний*) *ключ*.

Варто зауважити, що серед алгоритмів *асиметричної криптографії*, що використовуються в *блокчейн-проектах*, алгоритми *дискретного логарифмування на еліптичних кривих* мають найвищу, (а саме – *експоненціальну*) складність.

Тобто такі алгоритми є найбільш криптографічно-стійкими.

В мережі *блокчейн біткойн* використовується алгоритм *асиметричної криптографії дискретного логарифмування в групі точок еліптичної кривої (ECDSA)*.

Біткойн використовує дуже просту еліптичну криву, що визначається формулою:

$$y^2 = x^3 + 7.$$

Виявляється вибраних коефіцієнтів цілком достатньо, щоб забезпечити необхідний рівень складності задачі відновлення *секретного* ключа на основі *публічного*:

- Принаймні поки що невідомо *жодної вдалої спроби* зламання цього алгоритму.

4. Генерування ключів в мережі блокчейн біткойн.

Початок реального, практичного функціонування мережі *блокчейн біткойн* датується 3 січнем 2009 р. Саме цього дня Сатоші Накамото створив її перший (*вихідний*) блок. Дев'ятьма днями пізніше – 12 січня 2009 р. він же реалізував першу *біткойн-транзакцію*.

Подивимось детальніше, що за цим стоїть і на прикладі *блокчейн біткойна* проілюструємо, що потрібно для створення *блокчейн* і як він працює.

Що потрібно для створення *блокчейну*?

- Перш за все потрібні *учасники* системи (її *вузли*), між якими реалізуються транзакції.

Для того, щоб стати учасником системи, користувачу необхідно згенерувати для себе пару ключів:

- *Секретного* та
- *Відеритого*.

З цією метою він «скачує» програмне забезпечення системи «*Біткойн*», що знаходиться в *Інтернеті* у вільному доступі і натискає відповідну кнопку в інтерфейсі програми-клієнта:

- Ця програма випадковим чином генерує його 256-бітний *секретний* ключ.
- Потім, використовуючи його та названий вище «*алгоритм асиметричного шифрування*», за *конкретними формулами* обчислює *відкритий (публічний)* ключ такого розміру (256-бітний).

Таким чином ці два ключі жорстко між собою пов'язані.

- *Генер користувач має все необхідне, щоб стати учасником системи.*
- Підтвердженням присутності користувача в мережі, того, що він є окремим її вузлом, тобто *рівноправним суб'єктом* або *учасником* системи являється його *адреса*.

Підставою до формування адреси служить *відкритий* ключ, а її створення відбувається за наступним алгоритмом:

- Спочатку відкритий ключ проходить *попередньо* дві процедури хешування:
 - ✓ *Перша* – SHA-256;
 - ✓ *Друга* – MDS.

В результаті другої процедури його розмір скорочується з 256 до 160 біт.

- Цей *хеш* доповнюється двома типами службової інформації:
 - ✓ На початку додається *один байт*, що вказує ідентифікатор мережі: *основна* чи *тестова*.

Транзакцію неможливо відкликати:

- *Відправник крипто-активів не має права на помилку!*
 - Якщо адреса введена неправильно – кошти підуть «*в нікуди*».

Іншими словами, ніхто не зможе ними скористатися, оскільки не існуватиме відповідного *секретного* ключа.

Для запобігання цьому в мережі *блокчейн біткойн* існує попередження у вигляді *контрольної суми* адреси:

- ✓ Контрольна сума є частиною *хеши* останнього результату і додається в кінці у вигляді *чотирьох байтів*.
- Якщо відправник, вводячи адресу, припуститься *помилки* – система його *поінформує* про це.

Заключний крок в формуванні адреси – перетворення його в більш «зручний» для використання вигляд

- Початковий вигляд – блок даних в форматі 16-ричного коду за допомогою алгоритму «*Base58*» перетворюється в рядок цифр, малих та великих латинських літер.
- Отже *біткойн-адреса* представляється в форматі ASCII (*American Standard Code for Information Interchange* – американський стандарт коду для обміну інформації), за допомогою спеціалізованого кодування 58 буквено-цифрових символів.

Наприклад перша створена біткойн-адреса мала вигляд:

1A1zP1eP5QGefi2DMPTfTL5SLmv7Divfna44

- Отримавши адресу користувач стає *учасником системи*.

Але спочатку (*крім нього*) про це *ніхто не знає*, адже процедура формування біткойн-адреси відбувалася на його власному комп'ютері.

6. Як потрапити в чергу мережі блокчейн біткойн?

«*Старі*» учасники мережі довідаються про новий її «*вузол*» лише тоді, коли він розпочне «*активну*» діяльність, тобто участь в транзакціях.

- Для цього спочатку він мусить отримати на свою адресу *криптоза-соби*. (мати на своєму рахунку *криптоактиви*).

Потім він зможе відправляти їх на довільний вузол системи, і тоді про нього дізнаються всі, як про нового учасника мережі.

В мережі в умовах жорсткої конкурентної боротьби учасників системи відбувається формування нових *блоків транзакцій*.

- Приблизно протягом 10 хвилин відбувається створення нового блоку, в якому розміщено приблизно 4000 транзакцій.

Для практичної реалізації транзакції в *блокчейні* типу *біткойн* необхідно мати три «*інформаційні інструменти*»:

- ✓ Особистий *ключ* дебетової адреси (*біткойн-адреса*), тобто *секретний* ключ отримувача.

- ✓ Загальний *ключ* кредитової адреси, тобто *відкритий* ключ відправника.
- ✓ *Сума транзакції*, тобто відправник повинен мати невикористані входи на суму транзакції.

Якщо хтось з учасників має все це, то використовуючи програмне забезпечення він формує *зміст транзакції*, а система автоматично, використовуючи прямі поєднання між вузлами, розсилає цю інформацію по всій мережі.

➤ Таким чином реалізується принцип *колективного управління* та *колективного консенсусу*.

Отримавши інформацію кожен вузол здійснює її перевірку на «валідність». Ця перевірка передбачає наступне:

- Використовуючи закладені в системі принципи підрахунку «балансу» (сума «невитрачених входів» на адресі відправника), встановлюється, чи має він потрібні кошти.
- Щоб перевірити, чи має відправник *секретний* ключ від вузла, з якого знімаються активи, перевіряється його електронний підпис.

Для цього, як відомо, вистачить його *відкритого* ключа та математичних формул алгоритму побудови ЕЦП в системі.

➤ Якщо операція *успішно пройде* таку перевірку, то вона потрапить в *чергу*, на реалізацію а мережі.

7. «Жива» черга та «медпул».

Як такої «живої» черги (тобто черги, в якій дані обробляються в залежності від часу їх надходження) в мережі *блокчейн біткойн* не існує.

Головний спосіб емісії нових крипто-монет – це *нагорода* за створення нового блоку.

Кожен учасник, що конкурує в цьому змаганні, сам формує склад блоку і якщо виграє – отримає *всю нагороду*. А це:

- *Премія* за створення блоку;
- *Комісійні* із всіх транзакцій до нього включених.

Величину комісійних встановлює *відправник* намагаючись таким чином прискорити виконання своєї операції.

- ✓ Тому в мережі *біткойн* заявки впорядковуються за *величиною комісії* і така черга (*тимчасове сховище*) називається *тетруол* («*мемпул*»).

Для того, щоб створити блок, необхідно:

- Набрати транзакцій з *мемпула*, поки вистачає місця в блоці.

- На підставі відібраних операцій обчислити *кореневе значення дерева Меркла*.
- Використовуючи корінь Меркла та іншу службову інформацію сформувати заголовок блоку.
- Помістити в цей заголовок *хеш* заголовку попереднього блоку.

Після цього (з *технологічної* точки зору) блок готовий і його можна відправити в мережу для того, щоб всі інші її учасники включили його в *кінець* існуючого вже ланцюга блоків.

- Але всі ці завдання дуже прості і сучасний комп'ютер виконує їх миттєво.

Тому, якщо обмежитись тільки перерахованими завданнями, то в результаті практично *всі вузли* перетворюються в друкарки *біткойнів*:

- ✓ Багато з них почнуть одночасно пропонувати свої блоки;
- ✓ Виникнуть конфлікти між претендентами на включення нових блоків;
- ✓ Канали зв'язку будуть перенавантажені синхронізацією системи;
- ✓ Неможливо буде уникнути розгалужень ланцюга блоків, коли *одна частина* вузлів акцептуватиме *один блок*, а *друга – інший*.

Одним словом:

- Розпочнеться *повний хаос*, система втратить *цілісність*, а отже і *працездатність*.

З метою запобігти цьому в мережі блокчейн біткойн запроваджено принцип «*Proof-of-Work*» («*доведення роботи*»):

- Крім перерахованих завдань претенденту пропонується розв'язувати складну математичну задачу.
 - Її складність встановлюється таким чином, щоб черговий блок з'являвся (*в середньому*) кожні 10 хвилин.

Звісно, що при цьому конфліктні ситуації також будуть *можливі*, але *малоймовірні*.

8. Майнінг в мережі блокчейн біткойн.

В мережі Біткойн (по аналогії з добуванням *корисних копалин*) ця процедура називається «*майнінгом*».

- Майнінг – це *протокол (алгоритм) розподіленого та децентралізованого консенсусу*, що полягає в *дешифруванні* даних, яке відбувається *шляхом математичних обчислень*.

Це й пояснює походження назви «*криптовалюта*», адже щоб створити такі гроші необхідно пройти процес *дешифрування*.

Нік Сабо запозичив прийом «*доведення роботи*» («*Proof-of-Work*») для свого проекту «*Bit Gold*» у Адама Бека.

Розділ 4

Прогнозування кон'юнктури фінансових ринків

4.1. Прогнозування на основі часового ряду.

1. Загальна схема прогнозування на основі часового ряду. 2. Відображення довгострокових змін в часових рядах. 3. Тренд та тенденція розвитку. 4. Принципи та методи виділення тренду.

1. Загальна схема прогнозування на основі часового ряду.

Припустимо, що досліджуємо розвиток певного економічного явища у часовому інтервалі спостереження $t \in \{0, 1, 2, \dots, n\}$. Змінна Y описує динаміку цього явища, а

$$\{y_0, y_1, y_2, \dots, y_k, \dots, y_n\} = \{y_t, t = 0, 1, 2, \dots, n\},$$

часовий ряд, який представляє цю динаміку в інтервалі спостереження.

Задача полягає в тому, щоб спираючись на цей часовий ряд визначити *можливе* значення y^*_τ змінної Y в момент часу $\tau = n + s$, що належить до *майбутнього*.

Основою будь-якого прогнозування є встановлення *статистичних закономірностей*, яким підпорядкований напрямок та характер розвитку досліджуваного явища і які можна виявити, аналізуючи часовий ряд. Певні труднощі з визначенням прогнозованих значень створює складність структури часового ряду $\{y_t, t = 0, 1, 2, \dots, n\}$:

- Значення y_t є сумою декількох компонент *різної природи*, що «формують» часовий ряд та одночасно присутні в ньому.

Природа кожної складової значень $y_t, t = 0, 1, 2, \dots$, є різною і вимагає різних математичних засобів для свого аналізу. Тому процес побудови прогнозів на основі часових рядів зазвичай протікає наступним чином

- Проводиться *декомпозиція* часового ряду $y_t, t = 0, 1, 2, \dots$.

Першим кроком такої декомпозиції є встановлення того, які компоненти «можуть бути присутніми» в досліджуваному ряду.

Після визначення «складу» часового ряду, його значення $\{y_t, t = 0, 1, 2, \dots, n\}$ «розкладаються» на окремі компоненти.

- Наступний крок декомпозиції – це визначення *впливу кожної з цих компонент* на значення прогнозованої змінної.

На практиці це виглядає наступним чином.

- ✓ Основний «напрямок» розвитку досліджуваного явища визначає *функція тренду*.

Тому за допомогою відповідних методів в часовому ряді виділяється *тренд*, тобто будується функція тренду:

$$f(t), t \in \{0, 1, 2, \dots, n\}.$$

✓ Прогнозування «основного напрямку розвитку» досліджуваного явища відбувається шляхом екстраполяції функції тренду $f(t)$ в інтервал прогнозу $\tau = n + s$.

Іншими словами, обчислюється значення

$$f^*_{\tau} = f(\tau) = f(n + s)$$

функції тренду «поза» інтервалом спостереження в момент $\tau = n + s$, що належить до майбутнього. f^*_{τ} можна розглядати як «найбільш ймовірне» для змінної Y в цей момент.

використовуючи, тобто

Після цього слід внести необхідні «корективи» в отримане значення $f^*_{\tau} = f(\tau)$, враховуючи вплив на прогнозовану змінну Y інших компонентів часового ряду, а саме:

- Вплив на Y явища сезонності.
- Вплив на Y циклічності розвитку економічних явищ.
- Врахувати стохастичний характеру досліджуваного процесу, тобто вплив на Y випадкової компоненти.

До згладжування часових рядів, тобто при видаленні з них випадкових коливань, широко використовуються найпростіші механічні методи, зокрема метод середніх рухомих [2], [4], [5].

Статистичними засобами, що дозволяють врахувати вплив сезонних чинників (як адитивних, так і мультиплікативних) та внести до прогнозу необхідні корективи, є показники сезонності. При їх підрахунку використовується парна («центрована») середня рухома [2], [4], [5].

2. Відображення довгострокових змін в часових рядах.

Припустимо, що економічне явище, яке є предметом дослідження, можна описати за допомогою змінної Y . Згідно з визначенням, часовим рядом

$$\{y_0, y_1, y_2, \dots, y_T\}$$

для змінної Y називається послідовність її значень, впорядкована відносно одиниць часу з певного проміжку $t \in \{0, 1, 2, \dots, T\}$.

Як неодноразово підкреслювалось, кожне окреме значення

$$y_t, t = 0, 1, 2, \dots,$$

змінної Y , пов'язаної з явищем, що вивчається, зазвичай, є сумою багатьох компонент, які його формують. Отже структура значень y_t часового ряду може бути досить складною.

Визначення довгострокових закономірностей, притаманних явищу, що досліджується, потребує його спостереження в довгостроковій

перспективі, тобто загальна довжина (T) часового ряду повинна бути «значною». Тут головну роль відіграють *систематичні складові* часового ряду, такі, як: 1) *Постійний рівень*; 2) *Тренд*; та 3) *Циклічна складова*.

Тому, перш за все, дослідження довгострокових змін розпочинається з встановлення *математичної структури* окремих значень часових рядів, тобто *виділення окремих компонентів*, що містяться в цих значеннях.

➤ Моделі часових рядів використовуються тоді, коли досліджуване явище є *надто складним*, щоб його можна було вивчити за допомогою формальної *причинно-наслідкової аналітичної моделі*.

Складається ситуація, коли «*вартість*» побудови *економетричної моделі* для цього явища *непропорційно висока* порівняно з *технічним аналізом* відповідних часових рядів, тоді як «*якість*» аналітичної моделі не обов'язково буде «*кращою*» порівняно з моделлю часових рядів.

Назва «*технічний аналіз*» зумовлена насамперед тим, що основними інструментами цього аналізу є *різні типи діаграм і таблиць*. Коротко технічний аналіз можна визначити наступним чином:

➤ *Побудова та інтерпретацію* графіків на основі емпіричних даних про конкретні явища за періоди часу, який належать до *минулого*.

Ці графіки показують *динаміку* досліджуваного явища, враховуючи *всі фактори*, що на нього діють.

Аналізуючи їх переконаємось в слушності *основних принципів* та припущень технічного аналізу [4], зокрема:

- Припущення про те, що *динаміка розвитку природних явищ* – це *спрямований рух*;
- Розвиток природних явищ – *циклічний процес*, а хвиля динаміки *повторюється*.

3. *Тренд та тенденція розвитку.*

Поняття *тренду* та *тенденції* відіграють ключову роль в технічному аналізі та теорії часових рядів.

- Обидва ці поняття характеризують *систематичні, односторонні зміни* часового ряду, але вони *не тотожні*.

Уточнимо їх суть та взаємозв'язок, що між ними існує.

➤ Тренд характеризує *поточний напрямок* зміни досліджуваного явища.

Зазвичай існує *три типи* трендів:

- Рух *вгору* (в біржовій термінології - *бичачий тренд*);
- Відсутня *помітна* зміна, тобто *бічний рух*, що вказує на збереження *майже постійного рівня*;
- Рух *вниз* (в термінології фондової біржі – *ведмежий тренд*).

Існує відповідно також *три типи* тенденції:

- *Бичача;*
- *Бічна;*
- *Ведмежа.*

Тенденція визначається наступним чином:

- Враховуючи циклічний характер розвитку, *тенденція* буде залишатися *зростаючою* до тих пір, поки кожен наступний «пік» і кожне наступне «дно» графіка хвилі буде *вище* попереднього.

Іншими словами, *висхідна* тенденція повинна мати форму кривої з *послідовно зростаючими* локальними екстремальними значеннями: як *максимальними*, так і *мінімальними*.

- У випадку тенденції *спадкової* (до *зниження*) кожен наступний «пік» і кожне наступне «дно» графіка хвилі буде *нижчим* за попередній.

Одне з основних припущень щодо взаємозв'язку між поняттями «*тренд*» та «*тенденція*», можна сформулювати наступним чином:

Тренд рухається в тому ж самому напрямку до тих пір, поки *тенденція* не змінить свій напрямок на протилежний.

Отже в часових рядах з *математичної* точки зору:

- *Тренд* трактується як *певна функція часу*, що визначає *головний* напрям розвитку досліджуваного явища.

У багатьох випадках, (особливо це стосується *біржових* процесів), основною метою дослідження часових рядів, що описують відповідні явища, є знаходження в їх трендах *моментів «перелому»*, тобто:

- Моментів, в яких існуюча *тенденція* змінює свій напрямок.

Для того, щоб розв'язати сформульовану задачу, спочатку необхідно *розпізнати* та *виділити* в часовому ряді *тренд*.

- Це допоможе відрізнити звичайну проміжну *корекцію* основної *тенденції* від зміни її напрямку на зворотній, тобто *вгадувати* моменти зміни *напрямку* існуючої *тенденції*.

4. Принципи та методи виділення тренду.

Серед факторів, що формують досліджуване явище, крім *істотних* (основних, *постійних*) присутні також *неістотні* (*побічні, випадкові, непередбачувані*) чинники.

- Це є головною причиною того, що замість *тренду* (тобто *строго визначеної залежності* значень елементів часового ряду від часу) ми спостерігаємо *тенденцію розвитку* відповідного явища.

Коливання, спричинені *побічними* факторами, не здатні *змінити* основний напрямок розвитку явища, тобто *приховати* існуючий

тренд, однак ми спостерігаємо цей тренд *на фоні* різного роду коливань.

Оскільки перелік таких побічних причин може бути досить довгим, то і у часовому ряду може бути досить багато різних типів коливань. Крім того стохастичний характер цих коливань вимагає спеціальних математичних засобів їх формалізованого опису.

Як правило ці методи мають своє джерело в теорії ймовірності та математичній статистиці.

- Тому подібні коливання часто називають «*випадковою складовою*», або «*випадковими коливаннями*».

➤ Суть статистичних методів визначення тренду в часовому ряду полягає в тому, щоб *видалити* з нього всі *випадкові коливання*.

В математичній статистиці існує два типи методів визначення тренду: 1) *Аналітичні* методи; та 2) *Механічні* методи. Серед аналітичних необхідно, перш за все, назвати метод виділення тренду за допомогою причинно-наслідкової моделі *тенденції розвитку*, детально описаний в лабораторній роботі №6 (*підрозділи 3.10 – 3.13*).

В *причинно-наслідковій* моделі *випадкові коливання* мають вигляд *випадкової складової*. Тому видалення їх з часового ряду відбувається шляхом побудови на підставі емпіричних даних *економетричної моделі*.

Роль незалежної змінної (тобто *причини*) в цій моделі відіграє час. Для побудова моделі використовуються статистичні та математичні методи, а відповідна процедура виглядає наступним чином:

- Приймається конкретний *гіпотетичний* математичний вигляд моделі, тобто визначається *функція*, яка встановлює *залежність* значень елементів часового ряду *від часу*.
- За допомогою методів математичної статистики оцінюються необхідні *параметри* моделі з подальшою статистичною верифікацією отриманих результатів.

Технологія «*блокчейн*» та *цифрові гроші*, як новий сегментів фінансового ринку – це головний предмет досліджень цієї книги. Описуючи ймовірнісні та статистичні методи прогнозування кон'юнктури на цих ринках намагаємось підкреслити специфіку *криптовалют* та особливості *крипто ринку*. Одна з них – висока *волатильність цифрових грошей* (див. *підрозділ 2.7*). Тому перш ніж перейти до презентації *простих і ефективних* механічних методів «*згладжування*» емпіричних даних та *адаптивних* методів конструювання *оперативних* прогнозів, наведемо приклади прогнозування курсу *біткойна* та гривни за допомогою «*потужних*» *аналітичних* методів. Переконаємось в тому, як «*обережно*» необхідно застосувати ці методи на практиці, та який вплив на їх використання можуть мати «*специфічні особливості*» відповідних сегментів фінансового ринку.

4.2. Передбачення майбутніх подій та класифікація прогнозів.

1. Функції прогнозів.
2. Достовірність статистичного прогнозу.
3. Типи прогнозів.
4. Характер змін та типи прогнозів.

1. Функції прогнозів.

При обговоренні в підрозділі 2.1 базових понять теорії прогнозування йшлося, зокрема, про *нераціональне* та *раціональне* передбачення майбутнього.

- З *раціональними* передбаченням маємо справу тоді, коли рішення *щодо майбутніх* подій базуються на *інформації про минуле*, а прийняття цих рішень – це логічний процес переходу від *передумов* до *висновків*.

Необхідною умовою будь-якого передбачення майбутнього є знання минулих подій та відповідних закономірностей, яким вони підпорядковані. Популярним є наступний вислів:

«Прогноз вартий рівно стільки, скільки коштує інформація, на якій він базується».

Об'єм знань щодо прогнозованих явища постійно зростає, а це дозволяє сподіватися, що буде зростати і якість прогнозів.

- *Прогнозування* – це *раціональне, наукове передбачення* майбутніх подій. Результатом процесу *прогнозування* буде певне *рішення*, яке називаємо *«прогнозом»*.

Під прогнозом ми розуміємо *судження* про настання конкретної *події* у визначеному часі, що належить майбутньому (з точністю до *моменту* або *періоду*).

Прогнозування в суспільній та економічній сферах виконує ряд важливих функцій. Серед головних можна виділити наступні: *активуючу, інформаційну та підготовчу*.

Активуюча (чи *активізуюча*) функція означає спонукування людей до певних дій:

- Коли прогноз анонсує *корисні* для нас події, ми робимо все, щоб *сприяти* їх реалізації.
- Однак, коли ми оцінюємо подію, передбачену в прогнозі, як *несприятливу*, ми вживаємо заходів для протидії їй.

З активізуючою функцією тісно пов'язана *інформаційна* функція прогнозів. *Оголошення* прогнозів – це своєрідне *інформування* суспільство про майбутні зміни. Тим самим прогноз *готує* громадськість до цих змін та допомагає їх суспільному сприйняттю.

Беручи до уваги зміст розглянутих функцій, варто підкреслити, що прогнози самі по собі є *суспільними явищами*. Тобто разом з іншими явищами *ці прогнози* можуть впливати на *настання* або *ненастання* про-

гнозованих ними *подій*. Це, очевидно, ускладнює процес прогнозування в соціально-економічній сфері.

Однак головною серед трьох названих функція є *підготовча*. Вона означає, що прогнозування є *діяльністю*, що готує *інші види діяльності*.

➤ Основною ж метою економічного прогнозування є *підтримка процесів прийняття рішень*.

2. Достовірність статистичного прогнозу.

В центрі уваги досліджень цієї книги є поняття «*статистичного прогнозу*» та його «*практичне втілення*». Згідно з визначенням:

➤ Статистичним прогнозом називаємо кожне *судженням*, правдивість якого є *випадковою* подією, *ймовірність* якої відома і достатньо *висока* для практичних цілей.

Іншими словами «*статистичний прогноз*» – це *судження*, що характеризується такими властивостями:

- Сформульоване з використанням *досягнень науки*.
- Відноситься до *конкретного* майбутнього.
- Має можливість *емпіричного* підтвердження (перевірки).
- *Непевне*, але *прийнятне*.

Варто підкреслити найважливішу особливість статистичного прогнозування, яка відрізняє його від інших видів прогнозів, а також відрізняє процес «*прогнозування явищ*» від *процесу їх моделювання*», які є досить схожими між собою.

➤ Будь-який прогноз, крім судження про можливість певних подій у майбутньому, повинен містити також *оцінку ступеня довіри до нього*, звану *достовірністю прогнозу*.

Достовірність прогнозу можна охарактеризувати як *додатне дробове число*, *близьке до одиниці*, яке вказує значення *ймовірності істинності* судження, що розглядається як прогноз.

Наведене вище визначення статистичного прогнозу *безпосередньо* включає цей постулат, припускаючи, що *ймовірність події*, яка є прогнозом, *відома*.

З погляду на *достовірність* прогнозу виділяємо «*реалістичні*» прогнози, тобто такі, до яких користувач має «*високу довіру*». Тут варто зазначити, що, подібно до «*статистичних висновків*» у математичній статистиці, такі «*розпливчасті*» (нечіткі) поняття, як «*високий*», «*великий*», «*досить високий*», «*досить великий*» тощо, в залежності від ситуації потребують додаткової *кількісної специфікації* (тобто *уточнення*).

Наприклад, для виконання своїх активізаційної чи інформаційної функцій, прогноз не обов'язково повинен бути *реалістичним*.

Натомість підготовчу функцію можуть виконувати лише *реалістичні* прогнози. Рідко коли «споживач» прогнозу, тобто особа, яка приймає рішення, може сама зробити потрібний йому прогноз. Зазвичай вона доручає це прогнозісту – нині самі прогнози стали «товаром», який «виробляють» спеціалізовані компанії. Приймаючи рішення, що значною мірою буде базуватися на прогнозі, складеному кимось іншим, необхідно мати впевненість в його якості.

3. Критерії класифікації.

З погляду на спосіб визначення прогнозованої події, що залежить від характеру вираження стану змінної, що прогнозується, прогнози поділяються на *кількісні* та *якісні*.

- Якщо прогнозована подія є *станом якісної змінної* або *усно описаною* ситуацією, що стосується кількісної змінної, то такий прогноз називається *якісним*.
- Якщо предметом прогнозування є кількісна змінна, стан якої виражається в цифрах, то такий прогноз називається *кількісним*. Такий прогноз, в свою чергу, може бути двох видів: *точковим* або *інтервальним*.
 - Точковим прогнозом називаємо *число*, яке вважається *найкращою оцінкою* значення змінної прогнозування у визначеному часі, що належить майбутньому і на який будується прогноз.
 - Інтервальний прогноз – це *числовий інтервал*, який із задалегідь визначеною ймовірністю, що називається *достовірністю* прогнозу, містить невідоме значення прогнозованої змінної у визначеному часі, на який будується прогноз.

Цей інтервал відповідає попередньо встановленій *достовірності* прогнозу, а отже – залежить від неї. Тому *довжину* інтервалу можна використати для оцінювання *точності* прогнозу.

Наступним критерієм для класифікації прогнозів може бути *горизонт* прогнозування, тобто визначений у майбутньому час, на який будується прогноз. З цієї точки зору виділяють:

- Короткострокові;
- Середньострокові; та
- Довгострокові; прогнози.
 - Короткострокові прогнози припускають лише *незначні відхилення* від останніх показників.

Цей тип передбачень називають ще *оперативним* прогнозуванням. В економічному плануванні необхідність короткострокового прогнозування часто викликана затримками в отриманні необхідної *актуальної* інформації, що інколи змушує прогнозувати навіть *поточну ситуацію*. На практиці короткострокові прогнози, як правило, складаються на найближчі кілька

днів (або місяців), в залежності від характеру та масштабу явища, що досліджується.

- Середньостроковий прогноз передбачає такий часовий горизонт, впродовж якого може істотно змінитися характер розвитку явища, що вивчається.

В економічному плануванні середньостроковий період прогнозування може досягати кількох років, як правило – від року до трьох. За цей час з різних причин умови господарювання можуть змінитися, а тому проста екстраполяція існуючих тенденцій може призвести до серйозних помилок. плануванні

- Довгострокові прогнози зазвичай охоплюють період більше трьох років.

За цей період можуть відбутися значні зміни як для окремих компаній, так і для економіки в національному масштабі. Для компаній це може бути освоєння нових товарів, нових ринків, злиття з іншими компаніями тощо. Біль загальні – це демографічні зміни в країні, структурні зміни в економіці, нові напрямки на умови в міжнародних зв'язках, тощо.

4. Характер змін та типи прогнозів.

Таким чином, наведені міркування показують, що *безпосередньо час* не є основною ознакою поділу прогнозів на короткострокові, середньострокові та довгострокові. Тобто тривалість періоду, який охоплює прогноз, сам по собі не визначає тип прогнозу. а

➤ Про тип прогнозу свідчить *характер та суть змін*, які відбуваються за цей період з явищем, що досліджується.

Ці зміни ділимо на два типи: *кількісні та якісні*.

- До кількісних зараховуємо такі зміни, що відбуваються згідно з *раніше виявленою закономірністю*. Вони, як правило, виражаються у *збільшенні або зменшенні* значення змінної прогнозування.
- На відміну від кількісних, *якісні* зміни виражаються у *відхиленні* від попередніх закономірностей. Вони можуть стосуватися *зміни характеру зв'язків* між досліджуваними явищами, або зміни факторів, що впливають на них. В результаті цього виникають зміни *істотних властивостей* цих явищ.

Враховуючи ці зауваження можемо доповнити та уточнити характеристику введених типів прогнозів:

- Короткостроковим вважається прогноз на такий період часу, в якому відбуваються *лише кількісні зміни*;
- Середньостроковий прогноз охоплює період часу, протягом якого, крім *кількісних змін*, очікуються також *якісні зміни*.

➤ Довгостроковий прогноз стосується періоду часу, впродовж якого можуть відбутися як *кількісні*, так і *серйозні якісні* зміни.

Ці уточнення свідчать про те, що *тип прогнозу* визначається *розміром* об'єкта і *характером* явищ, що відбуваються в ньому.

- Чим *більший* об'єкт, тим більшою, суттєвішою буде його *«інерційність»*.

Тому прогнози на момент, рівновіддалений від *«тепер»*, можуть бути для одних об'єктів *короткостроковими*, а для інших – *довгостроковими*. Більш того, навіть в одному і тому ж об'єкті *одні явища* можуть змінюватися *швидко*, інші – *повільно*. Все це є свідченням *відносності* (релятивності) розглянутої класифікації.

Слід, однак, підкреслити, що визначення *типу змін*, які відбуваються в прогнозованому явищі, є особливо важливим з точки зору всього процесу прогнозування,

➤ Характер цих змін впливає на *вибір* відповідних *методів*, що в кінцевому результаті визначає *якість* отриманих прогнозів, тобто *успіх* чи *невдачу* прогностичної процедури.

Переважно більшість економічних процесів, зокрема явища фінансової сфери, неможливо адекватно описати за допомогою формальних *детермінованих* моделей. Ці явища по своїй суті мають стохастичний характер, тому *відповідними* методами їх аналізу є *статистичні* методи.

В *підрозділі 4.1* представлена загальна процедура прогнозування з використанням даних, які містить часовий ряд $\{y_t, t = 0, 1, 2, \dots, n\}$. Зверталось при цьому увага на певні пов'язані з цим труднощі. Підкреслювалось, що виникають вони, перш за все, з приводу складності структури значень економічного часового ряду, оскільки y_t – це *сума* декількох компонент *різної природи*.

Головною серед цих компонент є *основна* тенденція розвитку явища, що досліджується. Вплив на цю тенденцію чинників *сезонності*, *циклічності*, що притаманні розвитку економічних процесів, *«спотворює»* її *«ідеальне»* значення. А присутність в реальному суспільно-економічному середовищі незліченої кількості *непередбачуваних* факторів перетворює прогнозоване явище у *випадковий процес*. В моделях, що розглядаються, ці фактори об'єднуються в своєрідну *«випадкову»* змінну.

До статистичних зараховуємо також методи *стохастичної теорії прогнозу*. Ці методи відразу трактують часовий ряд як *випадковий процес*, що належить до певного (конкретного) їх класу Тому, спираючись на дуже розвинену та розбудовану сучасну *теорію випадкових процесів* вони дозволяють не тільки вирішувати проблеми *визначення прогнозів* та оцінки їх *точності*, а й дають можливість виявити *«приховані»* в аналізованих емпіричних даних *закономірності*. Це, в свою чергу, допомагає знаходити *оптимальні* рішення та оцінювати *ризик*, пов'язані з їх прийняттям.

4.3. Прогнози на основі моделі тенденції розвитку.

1. Деякі особливості розвитку економічних явищ.
2. ARMA – моделі.
3. Загальні принципи економетричного прогнозування.

1. Деякі особливості розвитку економічних явищ.

Нехай

$$\{y_t, t = 0, 1, 2, \dots, T\}$$

часовий ряд, що містить емпіричну інформацію про явище, яке досліджується. Знаємо, що кожне число y_t цього ряду це сума декількох компонент різної природи, що *можуть* бути присутніми в ньому. При цьому кожна з цих компонент, що «*формують*» значення y_t , вимагає різних математичних засобів для свого аналізу.

Варто однак підкреслити, що всі його компоненти не обов'язково повинні бути присутніми в часовому ряді одночасно. Оскільки, як це неодноразово підкреслювалось, часові ряди, що стосуються соціально-економічних явищ, за своєю природою є стохастичними, то крім *основної* тенденції розвитку явища, «*обов'язковою*» є лише *випадкова* складова.

Для соціально-економічних явищ характерними є дві наступні ситуації:

- Перша з них дістала назву «*простих прогнозів*» та стосується прогнозування на основі часових рядів, що містять *систематичну* складову у вигляді *тренду* та *випадкові* коливання.
- Друга – коли значення змінної, що спостерігається, коливаються навколо більш-менш постійного рівня.

Це означає, що часовий ряд крім *випадкової* складової містить, *систематичну* складову у вигляді *середнього рівня* прогнозовної змінної.

Тоді досить легко визначити прогноз для змінної, що вивчається:

- У першому випадку застосовується прогностична модель *тенденції розвитку*;
- У другому використовуються *адаптивні моделі* прогнозування.

Обидві розглянуті ситуації дуже схожі з точки зору *математичної структури* досліджуваних часових рядів. Значення y_t , які спостерігаються для чергових моментів $t \in \{1, 2, \dots, T\}$, містять дві складові:

$$y_t = f(t) + \xi_t, t = 1, 2, \dots, T.$$

Різниця полягає в тому, що у випадку застосування моделі тенденції розвитку, *зміни* в значенні y_t викликані трендом $f(t)$, є значно *більшими*, ніж випадкові флуктуації ξ_t . Тому на графіку значень часового ряду добре видно *форму* функції $f(t)$ і досить тривалі інтервали «*монотонності*» її

динаміки. Ширина «смуги точок» графіка, яка визначається величиною випадкових флуктуацій ξ_t , не може приховати цю «тенденцію».

Натомість у випадку адаптивних моделей коливання, спричинені систематичною складовою ряду $f(t)$, набагато менші та повільніші, ніж непередбачувані зміни ξ_t у значеннях досліджуваної змінної y_t . Результатом цього є те, графік часового ряду нагадує *нерегулярні* коливання значень досліджуваного явища навколо *більш-менш постійного* рівня.

Подібною буде також *процедура прогнозування*, яка використовується для обох описаних ситуацій. Метою *першого кроку* цієї процедури, яка називається *згладжуванням* даних, буде «усунення» випадкових флуктуацій ξ_t із значень y_t ряду. Різниця полягає в тому, що:

- У випадку застосування моделі *тенденції розвитку* буде використано один із основних аналітичних методів *згладжування* даних – «метод найменших квадратів».
- У випадку *адаптивної моделі* будуть застосовані механічні методи *згладжування*, або ж *комбінація* механічних із найпростішими аналітичними методами усунення випадкових флуктуацій ξ_t із значень y_t ряду.

2. ARMA – моделі.

В практиці *економічного планування* на базі часових рядів, крім описаних вище схем, широкого розповсюдження здобули також методи *стохастичної теорії прогнозу*. Ці методи трактують часовий ряд як *випадковий процес*, що належить до певного (конкретного) їх класу. Найпоширенішими математичними моделями для *економічних* явищ є моделі, побудовані на основі *стаціонарних* випадкових процесів. Серед них можна виділити наступні:

- AR-моделі, побудовані на основі процесів *авторегресії*,
- MA-моделі, побудовані на основі процесів *ковзного середнього*,
- ARMA-моделі, тобто «поєднання», чи точніше – комбінація AR та MA моделей.

Спираючись на досвід практичних застосувань можна впевнено стверджувати, що в багатьох випадках ARMA-моделі є *оптимальними* методами визначення прогнозів. Г. Боксу та Г. Дженкінсу (див. [8]) вдалося поєднати кілька існуючих напрямків аналізу явищ за допомогою часових рядів і створити дуже ефективну та корисну з точки зору прогнозування методологію. Завдяки наявності комп'ютерів та широкому розповсюдженні відповідного програмного забезпечення, *методи Бокса-Дженкінса* стали основою сучасної теорії стохастичного прогнозу. З одно-

го боку, вони гарантують *досить високу точність*, тобто високу *якість* отриманих прогнозів, а з іншого – *дуже дешеві та доступні*.

3. Загальні принципи економетричного прогнозування.

Згладжування даних часового ряду аналітичним методом означає побудову на його підставі *економетричної* моделі:

$$y_t^* = f(t), t = 1, 2, \dots, T,$$

яка в цьому випадку називається *моделлю тенденції розвитку*, оскільки в якості «*фіктивної*» незалежної змінної в ній виступає час (t). Тому описану схему конструювання прогнозів з використанням моделі *тенденції розвитку* можна розглядати, як частковий випадок загальної процедури *економетричного* прогнозування (див. [2], [3]).

Припустимо, що маємо справу з часовим рядом $\{y_t, t = 1, 2, \dots, T\}$, що містить дві складові:

$$y_t = f(t) + \xi_t, t = 1, 2, \dots, T,$$

систематичну складову у вигляді тренду або тенденція розвитку $f(t)$ і випадкові коливання ξ_t . Форма функції $f(t)$ визначає аналітичний вигляд моделі. Випадкові коливання ξ_t ряду $\{y_t, t = 1, 2, \dots, T\}$ виступають в ролі *випадкової складової* (див. [підрозділи 1.2 та 1.8](#)), наявність якої є *характеристичною* ознакою економетричної моделі.

Процес прогнозування (див. [підрозділ 2. 1](#)), включає *дві фази*: 1) *діагностику* минулого та 2) *визначення* майбутнього. Обробка даних про минуле у випадку моделі тенденція розвитку (тобто діагностика минулого) здійснюється шляхом вибору *аналітичного вигляду* $f(t)$ функції тренду та визначення *оцінок її параметрів*.

- Задача визначення *функції тренду* $f(t)$ називається згладжуванням часового ряду $\{y_t, t = 1, 2, \dots, T\}$.

Ця функція повинна «*найкращим*» чином (з огляду на прийнятні критерії *оптимальності*) відповідати («*пасувати*») значенням $\{y_t, t = 1, 2, \dots, T\}$ часового ряду прогнозованої змінної.

Ключову роль при формулюванні гіпотез щодо аналітичного вигляду функції тренду $f(t)$ відіграє *графічний* метод, який полягає в аналізі графіка точок $\{(t, y_t), t = 1, 2, \dots, T\}$ часового ряду. Сугестивна візуальна оцінка графіка часового ряду, врахована при виборі функції тренду $f(t)$, створює *емпіричні передумови* для цього вибору.

Крім того сформульовані гіпотези щодо форми функції тренду $f(t)$ повинні також ґрунтуватися на *теоретичних* або *дедуктивних* передумовах, що стосуються як *теоретичного аналізу* явища, що розглядається, так і «*механізму можливого розвитку*» прогнозної змінної в часі.

Щоб перейти від діагностики минулого до визначення прогнозу, потрібно скористатися *якимось правилом прогнозування*. Найчастіше при визначенні прогнозів на основі моделі *тенденції розвитку* використовується так зване «*базове*» правило економетричного прогнозування.

Згідно з цим правилом, *прогноз* – це *майбутнє* значення прогнозованої змінної, при умові, що модель буде *актуальною* в *момент часу*, для якого зроблено цей прогноз.

Іншими словами, для того, щоб використати модель для побудови прогнозу, повинні виконуватись наступні припущення:

- а). Стабільність структурних зв'язків у часі, тобто як *аналітична* форма моделі, так і значення її параметрів не будуть змінюватися в інтервалі часу, для якого визначається прогноз;
- б). Стійкість (*незмінність*) *стохастичної структури* моделі, тобто розподілу ймовірностей випадкових флуктуацій.

Визначення. *Простим прогнозом* називається прогноз, отриманий на основі моделі тенденції розвитку з використанням «*базового правила економетричного прогнозування*».

Таким чином, прогноз y_{τ}^* майбутнього значення y_{τ} прогнозованої змінної Y на момент прогнозування ($\tau = T + s$) отримується шляхом екстраполяції функції тренду $f(t)$, тобто шляхом підстановки «*часової змінної*» τ , на яку визначається прогноз, у функцію $f(t)$: $y_{\tau}^* = f(\tau)$, $\tau = T + s$.

Визначення. Значення $y_{\tau}^* = f(\tau)$ називається *точковим прогнозом* змінної прогнозування Y , тобто *найкращою оцінкою* її значення в моменті прогнозування ($\tau = T + s$).

Модель тенденції розвитку можна використовувати як інструмент прогнозування лише тоді, коли виконуються зазначені вище припущення а). б). для цієї моделі. Треба розуміти, що навіть *виконання* цих вимог *не гарантує* абсолютної точності прогнозів, отриманих на основі цієї моделі. Статистичний прогноз ніколи не буває *певним*, він є тільки *вірогідним*. Тому, подібно як і у випадку параметричного оцінювання, постає проблема визначення *точності* отриманого точкового прогнозу y_{τ}^* та оцінювання *ризиків* прийняття *хибних висновків* на його основі. З метою вирішення цих задач будується інтервальний прогноз.

Визначення. Інтервальним прогнозом називається числовий інтервал $[d_{\tau}^*, g_{\tau}^*]$, який із заздалегідь визначеною ймовірністю β , яка називається *достовірністю* прогнозу, містить в собі невідоме майбутнє значення y_{τ} прогнозованої змінної Y на момент прогнозування $\tau = T + s$:

$$P\{d_{\tau}^* < y_{\tau} < g_{\tau}^*\} = \beta, \tau = T + s.$$

Очевидно, що для визначення інтервального прогнозу $[d_{\tau}^*, g_{\tau}^*]$ необхідно знати *розподіл ймовірностей* значення y_{τ} змінної прогнозування Y . Зважаючи на «*конструкцію*» $y_t = f(t) + \xi_t$ значень досліджуваного часового ряду, це означає необхідність визначення його *стохастичної структури*, тобто *розподілу ймовірностей* випадкових коливань ξ_t . З метою висвітлити виникаючих проблеми та окреслення можливих шляхів для їх вирішення розглянемо кілька конкретних прикладів.

4.4. Прогнозування курсу біткойна та гривні (лінійна модель): приклади та завдання для самоконтролю.

Економетрико-статистичні методи в дослідженні економічних процесів

1. Побудова прогностичної моделі тенденції розвитку. 2. Лінія регресії моделі: (історичний прогноз). 3. Точковий прогноз в інтервалі емпіричної верифікації. 4. Графічна ілюстрація. 5. Прогностична модель тенденції розвитку для курсу гривні.

Перш ніж перейти до розгляду прикладу наведемо цікаву інформацію:

➤ Сьогодні, **16.12.2024**. (коли пишеться цей підрозділ) курс біткойна по відношенню до долара США досягнув свого нового рекорду:

106 000 \$ за 1 біткойн!

Приклад 1. Наступні числові дані представляють курсу біткойна по відношенню до долара США з 1.01.2021 по 30.01.2021.

01.01.	02.01.	03.01.	04.01.	05.01.	06.01.	07.01.	08.01.	09.01.	10.01.
29374	32127	32782	31971	33992	36824	39371	40797	40254	38356
11.01.	12.01.	13.01.	14.01.	15.01.	16.01.	17.01.	18.01.	19.01.	20.01.
35566	33922	37316	39187	36825	36178	35791	36630	36069	35547
21.01.	22.01.	23.01.	24.01.	25.01.	26.01.	27.01.	28.01.	29.01.	30.01.
30825	33005	32067	32289	32366	32569	30432	33466	34316	34269

Необхідно побудувати лінійну прогностичну модель тенденції розвитку $V_t = b + a \cdot t + \xi_t$, $t = 1, 2, \dots, T$, та дослідити її властивості.

1. Побудова прогностичної моделі тенденції розвитку.

Числові дані наведені в цій таблиці утворюють часовий ряд,

$$\{V_1, V_2, \dots, V_n\} = \{V_t, t = 1, 2, \dots, 20\}, T = 30,$$

що представляє курсу біткойна протягом n днів ($t = 1, 2, \dots, 30$).

1.(а). Доступні спостереження часового ряду поділити на дві частини:

$$\{1, 2, \dots, T\} = \{1, 2, \dots, n\} \cup \{n + 1, n + 2, \dots, n + S\}, T = 30; n = 20, S = 10.$$

$\{1, 2, \dots, n\}$ – інтервал побудови моделі; $\{n + 1, n + 2, \dots, T\}$ – інтервал емпіричної перевірки прогнозу; наступним чином: $T = 30; n = 20; S = 10$.

1.(б). Побудувати в аркуші «Excel» графік точок

$$\{(1, V_1), (2, V_2), \dots, (n, V_n)\} = \{(t, V_t), t = 1, 2, \dots, n\}, (\text{Ряд } 1).$$

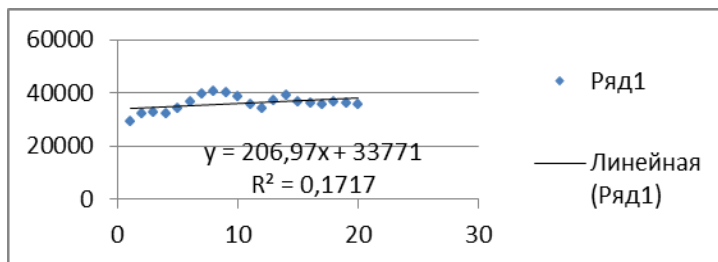


Рис. 1.

що представляють *числові дані* з інтервалу побудови прогностичної моделі.

1.(в). Використовуючи опцію «*Формат лінії тренду*» аркушу «*Excel*», додати до збудованого графіка теоретичну модель, (Лінійна (Ряд 1)) а також знайти *статистичні оцінки* $\{a^*, b^*\}$ для *структурних параметрів* моделі і числове значення множника детермінації R^2 .

Відповідь: Рис. 1. $y = 206,97x + 33771; R^2 = 0,1717$.

1.(г). Використовуючи емпіричні дані моделі $\{(t, V_t), t = 1, 2, \dots, n\}$ і застосовуючи функцію „*ЛІНІЙН*” аркушу «*Excel*», знайти значення $\{a^*, b^*\}$ оцінок МНК для структурних параметрів моделі та числове значення множника детермінації R^2 .

Відповідь: Функція „*ЛІНІЙН*”

a^*	206,97	33771,2	b^*
$S^*(a)$	107,15	1283,59	$S^*(b)$
R^{*2}	0,1717	2763,2	σ^*

2. Лінія регресії моделі: (історичний прогноз).

2.(а). Використовуючи побудовану лінійну модель тенденції розвитку побудувати лінію регресії моделі, тобто обчислити теоретичні значення $\{(t, V_t^*), t = 1, 2, \dots, n\}$ моделі: $V_t^* = b^* + a^* \cdot t, t = 1, 2, \dots, n$.

2.(б). Обчислити теоретичні значення моделі $\{(t, V_t^*), t = 1, 2, \dots, n\}$, (які називають також «історичним прогнозом») використовуючи для цього функції „*ТЕНДЕНЦІЯ*” аркушу «*Excel*».

Відповідь:

$V_{*1} \approx 33978,17; V_{*2} \approx 34185,14; V_{*3} \approx 34392,1; V_{*4} \approx 34599,07; V_{*5} \approx 34806,04;$
 $V_{*6} \approx 35013,01; V_{*7} \approx 35219,98; V_{*8} \approx 35426,95; V_{*9} \approx 35633,92; V_{*10} \approx 35840,89;$
 $V_{*11} \approx 36047,86; V_{*12} \approx 36254,83; V_{*13} \approx 36461,8; V_{*14} \approx 36668,77; V_{*15} \approx 36875,74;$
 $V_{*16} \approx 37082,71; V_{*17} \approx 37289,68; V_{*18} \approx 37496,65; V_{*19} \approx 37703,62; V_{*20} \approx 37910,59.$

3. Точковий прогноз в інтервалі емпіричної верифікації.

3.(а). Використовуючи побудовану лінійну модель тенденції розвитку визначити *точковий* прогноз $\{(t, V_t^*), t = n + 1, n + 2, \dots, n + S = T\}$ змінної V_t в інтервалі емпіричної верифікації, тобто інтервал, для якого значення $\{V_{n+1}, V_{n+2}, \dots, V_T\}$ часового ряду відомі.

3.(б). Визначити прогнозовані значення $\{(t, V_t^*), t = n + 1, n + 2, \dots, T\}$ змінної V_t в інтервалі емпіричної верифікації, використовуючи для цього функції „*ТЕНДЕНЦІЯ*” аркушу «*Excel*».

Відповідь:

$V_{*21} \approx 38117,56; V_{*22} \approx 38324,53; V_{*23} \approx 38531,49; V_{*24} \approx 38738,46; V_{*25} \approx 38945,43;$
 $V_{*26} \approx 39152,4; V_{*27} \approx 39359,37; V_{*28} \approx 39566,34; V_{*29} \approx 39773,31; V_{*30} \approx 39980,28.$

4. Графічна ілюстрація.

4.(а). Побудувати в аркуші «*Excel*» графік точок

$$\{(1, V_1), (2, V_2), \dots, (n, V_n)\},$$

що представляють *числові дані моделі* $\{(t, V)_t, t = 1, 2, \dots, n\}$ з інтервалу побудови прогностичної моделі. (Ряд 1)

4.(б). До побудованого графіку додати отримані в завданні 2.(а) теоретичні значення моделі

$$\{(1, V^*_1), (2, V^*_2), \dots, (n, V^*_n)\} = \{(t, V^*_t), t = 1, 2, \dots, n\}. \text{ (Ряд 2).}$$

4.(в). Додати до побудованого графіку отриманий в завданні 3.(а) *точковий прогноз*

$$\{(t, V^*_t), t = n + 1, n + 2, \dots, n + S = T\}$$

змінної V_t в *інтервалі емпіричної верифікації*, тобто інтервал, для якого значення $\{V_{n+1}, V_{n+2}, \dots, V_T\}$ часового ряду відомі. (Ряд 3)

4.(г). Додати до побудованого графіку відомі значення

$$\{(n + 1, V_{n+1}), (n + 2, V_{n+2}), \dots, (T, V_T)\} = \{(t, V)_t, t = n + 1, n + 2, \dots, T\},$$

часового ряду (Ряд 4).

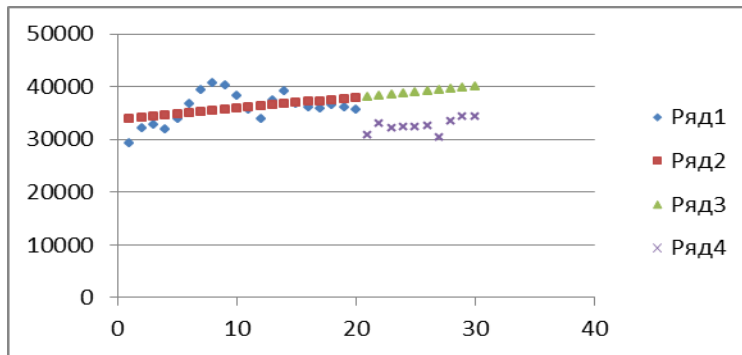


Рис. 2.

Відповідь: Рис. 2.

Отриманий малюнок є яскравою ілюстрацією того, що прогнози, отримані з використанням *моделі тенденції розвитку*, не є «найкращим» розв'язанням задачі, яка розглядалася в даному прикладі.

- Побудована з дотриманням всіх формальних математичних вимог модель очевидним чином не є відповідною в цій ситуації, оскільки «не змогла вгадати» реального напрямку розвитку явища, що нас цікавить. Однак причини цього не пов'язані з властивостями самої моделі: її *неефективністю* чи іншими *вадами*. Невластивим був *вибір* саме цієї моделі в ситуації, коли необхідно спрогнозувати динаміку ринкової ціни біткойна. Криптовалюта є новітнім «наддержавним» явищем в світових фінансах, яке не отримало ще свого ґрунтового вивчення та аналізу з точки зору

економічної науки. Несхожість до «традиційних», існуючих віддавна фінансових інструментів та специфічні властивості цього незвичайного активу, очевидним чином впливають на особливості крипто-ринку.

- Одна з таких особливостей – висока волатильність цифрових грошей та велика нестабільність їх валютного курсу.

Сучасний крипториннок – це вже окремих сегмент фінансового ринку, що інтенсивно розвивається. Його поведінка в значній мірі є непередбачуваною – тому вимагає нових засобів (втім і математичних) для свого вивчення. Ринкові курси криптовалют суттєво залежать від багатьох випадкових чинників, обставин та подій найрізноманітнішої природи. Все це має безпосередній вплив на вибір «відповідних» методів вивчення та прогнозування кон'юнктури ринків цифрових грошей.

Розглянутий приклад – це конкретна ілюстрація наведених зауважень. Часовий ряд, що складається з $T = n + S = 30$ спостережень, був поділений на дві частини:

- Інтервал (довжини n) побудови моделі: $t \in \{1, 2, \dots, n\}$,
- Інтервал (довжини S) емпіричної перевірки цієї моделі:

$$t \in \{n + 1, n + 2, \dots, n + S\}.$$

Дотримуючись рекомендованих теорією «пропорцій поділу», ми зробили це наступним чином: $n = 20$, $S = 10$.

В дійсності трапилось так, що в момент $n = 20$, тобто на «межі» між цими інтервалами, відбувся стрімкий «обвалу» курсу біткоїна:

$$V_{20} = 35547; V_{21} = 30825.$$

Внаслідок цього отриманий прогноз (Ряд 3) суттєво відрізняється від фактичного курсу (зафіксованих в дійсності значень) біткоїна (Ряд 4).

5. Прогностична модель тенденції розвитку для курсу гривні.

Розглянемо ще один приклад, а саме проведемо аналогічні дослідження для динаміки курсу гривни по відношенню до долара США за той самий період з 1.01.2021 по 30.01.2021.

Переконаємось в тому, що для передбачення динаміки курсу гривни прогностична модель тенденції розвитку також не буде «дуже вдалою». Однак причини «невідповідності» моделі у випадку гривни та у випадку біткоїна є цілком протилежними:

- Якщо у випадку біткоїна причиною була надмірна «волатильність» його курсу в інтервалі побудови прогностичної моделі, то у випадку гривни причиною була практична відсутність змінності її ринкової вартості в цьому інтервалі.

Наслідком цього було те, що формальна математична модель «потрапувала» випадкові (тобто несуттєві, різно-керункові) вагання курсу гривни навколо «більш-мени» сталого рівня, як «головний напрям

мок» зміни його нотувань. В результаті – *невідповідний* прогноз майбутніх значень.

Приклад 2. Провести дослідження динаміки курсу гривни по відношенню до долару США з 1.01.2021 по 30.01.2021, (аналогічні до тих, що проводились в **прикладі 1** стосовно біткоіна).

Відповідні числові дані наведені в наступній таблиці.

01.01.	02.01.	03.01.	04.01.	05.01.	06.01.	07.01.	08.01.	09.01.	10.01.
28,27	28,27	28,27	28,27	28,43	28,403	28,403	28,403	28,403	28,403
11.01.	12.01.	13.01.	14.01.	15.01.	16.01.	17.01.	18.01.	19.01.	20.01.
28,28	28,204	28,04	27,97	28,06	28,05	28,05	28,05	28,19	28,15
21.01.	22.01.	23.01.	24.01.	25.01.	26.01.	27.01.	28.01.	29.01.	30.01.
28,203	28,25	28,26	28,26	28,16	28,17	28,15	28,16	28,19	28,19

На підставі цих даних необхідно побудувати *лінійну прогностичну модель тенденції розвитку*

$$V_t = b + a \cdot t + \xi_t, t = 1, 2, \dots, T.$$

та дослідити її властивості.

1. Побудова прогностичної моделі тенденції розвитку.

Числові дані наведені в цій таблиці утворюють часовий ряд,

$$\{V_1, V_2, \dots, V_n\} = \{V_t, t = 1, 2, \dots, 20\}, T = 30,$$

що представляє курсу біткойна протягом n днів ($t = 1, 2, \dots, 30$).

1.(а). Доступні спостереження часового ряду поділити на дві частини:

$$\{1, 2, \dots, T\} = \{1, 2, \dots, n\} \cup \{n + 1, n + 2, \dots, n + S\},$$

$\{1, 2, \dots, n\}$ – інтервал *побудови* прогностичної моделі;

$\{n + 1, n + 2, \dots, T\}$ – інтервал *емпіричної перевірки* прогнозу; наступним чином:

$$T = 30; n = 20 \quad S = 10.$$

1.(б). Побудувати в аркуші «Excel» графік точок

$$\{(1, V_1), (2, V_2), \dots, (n, V_n)\} = \{(t, V_t), t = 1, 2, \dots, n\},$$

що представляють *дані* з інтервалу побудови прогностичної моделі.

1.(в). Використовуючи опцію «*Формат лінії тренду*» аркушу «*Excel*», додати до збудованого графіка теоретичну модель, а також знайти *статистичні оцінки* $\{a^*, b^*\}$ для *структурних параметрів* моделі і числове значення множника детермінації R^2 .

1.(г). Використовуючи *емпіричні дані* моделі $\{(t, V_t), t = 1, 2, \dots, n\}$ і застосовуючи функцію „*ЛІНІЙН*” аркушу «*Excel*», знайти значення $\{a^*, b^*\}$ оцінок МНК для *структурних параметрів* моделі та числове значення множника детермінації R^2 .

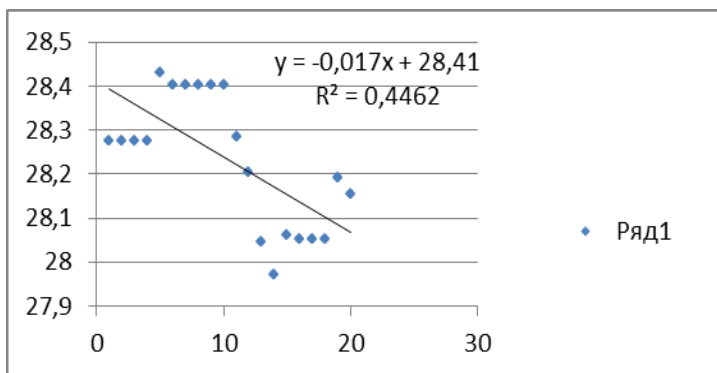


Рис. 3.

Відповідь: Рис. 3. Функція „ЛІНІЙН”

a^*	-0,01704	28,4096	b^*
$S^*(a)$	0,00448	0,05361	$S^*(b)$
R^{*2}	0,44621	0,1154	σ^*

2. Лінія регресії моделі: (історичний прогноз).

2.(а). Використовуючи побудовану лінійну модель тенденції розвитку побудувати лінію регресії моделі, тобто обчислити теоретичні значення $\{(t, V^*_t), t = 1, 2, \dots, n\}$ моделі:

$$V^*_t = b^* + a^* \cdot t, t = 1, 2, \dots, n.$$

2.(б). Обчислити теоретичні значення моделі $\{(t, V^*_t), t = 1, 2, \dots, n\}$, (які називають також «історичним прогнозом») використовуючи для цього функції „ТЕНДЕНЦІЯ” аркушу «Excel».

Відповідь:

$$V^*_1 \approx 28,39; V^*_2 \approx 28,38; V^*_3 \approx 28,36; V^*_4 \approx 28,34; V^*_5 \approx 28,32; \\ V^*_6 \approx 28,31; V^*_7 \approx 28,29; V^*_8 \approx 28,27; V^*_9 \approx 28,26; V^*_{10} \approx 28,24; \\ V^*_{11} \approx 28,22; V^*_{12} \approx 28,21; V^*_{13} \approx 28,19; V^*_{14} \approx 28,17; V^*_{15} \approx 28,15; \\ V^*_{16} \approx 28,14; V^*_{17} \approx 28,12; V^*_{18} \approx 28,1; V^*_{19} \approx 28,09; V^*_{20} \approx 28,07.$$

3. Точковий прогноз в інтервалі емпіричної верифікації.

3.(а). Використовуючи побудовану лінійну модель тенденції розвитку визначити точковий прогноз $\{(t, V^*_t), t = n + 1, n + 2, \dots, n + S = T\}$ змінної V_t в інтервалі емпіричної верифікації, тобто інтервал, для якого значення $\{V_{n+1}, V_{n+2}, \dots, V_T\}$ часового ряду відомі.

3.(б). Визначити прогнозовані значення $\{(t, V^*_t), t = n + 1, n + 2, \dots, T\}$ змінної V_t в інтервалі емпіричної верифікації, використовуючи для цього функції „ТЕНДЕНЦІЯ” аркушу «Excel».

Відповідь:

$$V^*_{21} \approx 28,05; V^*_{22} \approx 28,03; V^*_{23} \approx 28,02; V^*_{24} \approx 28; V^*_{25} \approx 27,98; \\ V^*_{26} \approx 27,97; V^*_{27} \approx 27,95; V^*_{28} \approx 27,93; V^*_{29} \approx 27,92; V^*_{30} \approx 27,9.$$

4. Графічна ілюстрація.

4.(а). Побудувати в аркуші «**Excel**» графік точок

$$\{(1, V_1), (2, V_2), \dots, (n, V_n)\},$$

що представляють *числові дані моделі* $\{(t, V)_t, t = 1, 2, \dots, n\}$ з інтервалу побудови прогностичної моделі. (Ряд 1)

4.(б). До побудованого графіку додати отримані в завданні 2.(а) теоретичні значення моделі

$$\{(1, V^*_1), (2, V^*_2), \dots, (n, V^*_n)\} = \{(t, V^*_t), t = 1, 2, \dots, n\}. \text{ (Ряд 2).}$$

4.(в). Додати до побудованого графіку отриманий в завданні 3.(а) *точковий* прогноз

$$\{(t, V^*_t), t = n + 1, n + 2, \dots, n + S = T\}$$

змінної V_t в *інтервалі емпіричної верифікації*, тобто інтервал, для якого значення $\{V_{n+1}, V_{n+2}, \dots, V_T\}$ часового ряду відомі. (Ряд 3)

4.(г). Додати до побудованого графіку відомі значення

$$\{(n + 1, V_{n+1}), (n + 2, V_{n+2}), \dots, (T, V_T)\} = \{(t, V)_t, t = n + 1, n + 2, \dots, T\},$$

часового ряду (Ряд 4).

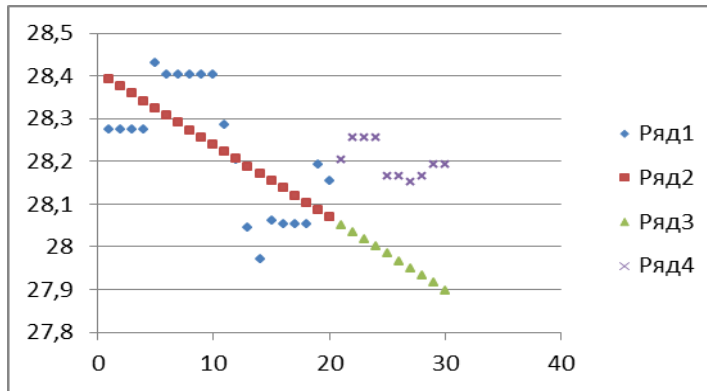


Рис. 4.

Відповідь: Рис. 4.

Подібно як і у випадку біткойна бачимо, що *прогностична модель тенденції розвитку* не є «*ефективним*» інструментом дослідження динаміки курсу гривни.

- Приведений Рис. 4. показує, що як в інтервалі *побудови* прогностичної моделі $t \in \{1, 2, \dots, 20\}$, так і в інтервалі *емпіричної перевірки* прогнозу $t \in \{21, 22, \dots, 30\}$, вартість гривни *несуттєво* вагається навколо «*більш-менш*» сталого рівня $V_{20} = 28,2$.

Формальна математична модель «*трактує*» випадкові (тобто *різно-керункові*) коливання в інтервалі $t \in \{1, 2, \dots, 20\}$, як «*головний напрям*» розвитку. В результаті – *невідповідний* прогноз: прогнозовані значення курсу гривни (Ряд 3) суттєво відрізняються від фактичних їх значень (Ряд 4).

4.5. Механічні методи згладжування часових рядів.

1. Механічні методи виділення тренду. 2. Візуальний аналіз графіка часового ряду. 3. Ковзне середнє. 4. Тренд на тлі випадкових коливань.

1. Механічні методи виділення тренду.

Розглянемо найпростіші методи виділення тренду, що застосовуються під час попередньої обробки часових рядів. Це методи, які зазвичай зараховуються до *описової статистики*:

- ✓ Графічний метод; та
- ✓ Метод середніх рухомих.

Простота цих методів, і в той же час, досить висока ефективність, роблять їх дуже популярними і вони часто використовуються на практиці. Пояснимо їх суть.

Графічний метод.

Припустимо, у нас є часовий ряд:

$$\{y_0, y_1, y_2, \dots, y_k, \dots, y_T\}$$

Часовий ряд можна трактувати як стохастичний процес y_t , $t = 0, 1, 2, \dots, T$, а його значення $\{y_0, y_1, y_2, \dots, y_T\}$, які спостерігались у часовому інтервалі:

$$t \in \{0, 1, 2, \dots, T\},$$

можна розглядати як функцію незалежної змінної $t = 0, 1, 2, \dots, T$. Тому ми завжди можемо побудувати графік відповідних точок

$$\{(t, y_t), t = 0, 1, 2, \dots, T\}$$

в системі координат tOY .

- Будемо вважати, що в певному *під-інтервалі* $[t_1, t_2]$ інтервалу

$$t \in \{0, 1, 2, \dots, T\}$$

існує *бичачий тренд* (іншими словами – «*рух вгору*») якщо ламана лінія, що з'єднує точки: $\{(t, y_t), t_1 \leq t \leq t_2\}$, демонструє *зростаючу тенденцію*,

Тобто в *під-інтервалі* $[t_1, t_2]$ кожен наступний «*пик*» і кожне наступне «*дно*» цього графіка *вищі*, ніж попередні.

- Будемо вважати, що в певному *під-інтервалі* $[t_1, t_2]$ інтервалу

$$t \in \{0, 1, 2, \dots, T\}$$

існує *ведмежий тренд* (іншими словами – «*рух вниз*») якщо ламана лінія, що з'єднує точки: $\{(t, y_t), t_1 \leq t \leq t_2\}$, демонструє *спадну тенденцію*,

Тобто в *під-інтервалі* $[t_1, t_2]$ кожен наступний «*пик*» і кожне наступне «*дно*» цього графіка *нижчі*, ніж попередні.

- Будемо вважати, що в певному *під-інтервалі* $[t_1, t_2]$ інтервалу

$$t \in \{1, 2, \dots, T\}$$

існує *бічний тренд*, якщо ламана лінія, що з'єднує точки: $\{(t, y_t), t_1 \leq t \leq t_2\}$, підтримує «*майже постійний*» рівень і має форму *нерегулярних* коливань.

Тобто в *під-інтервалі* $[t_1, t_2]$ графік «*коливається*» навколо *більш-менш* постійного рівня, не виявляючи при цьому «*помітної закономірності*».

Графічний метод виділення тренду полягає у такому проведенні *від руки* «*плавної лінії*» між точками $\{(t, y_t), t = 0, 1, 2, \dots, T\}$ графіку часового ряду, щоб вона була розташована «*максимально близько*» до них.

Побудована таким чином лінія може трактуватися як така:

✓ *Що найбільше відповідає загальній тенденції розвитку.*

Не приймаючи до уваги при цьому випадкові коливання в окремі моменти з досліджуваного періоду. Іншими словами – *усуваючи* із часового ряду *випадкові коливання*, тим самим – «*згладжуючи*» його.

2. Візуальний аналіз графіка часового ряду.

Описуючи процедуру декомпозиції часових рядів ми зазначали, що *візуальна оцінка* графіка часових рядів є важливою частиною його аналізу. У багатьох випадках за допомогою графіка ми робимо *вступну (попередню) ідентифікацію* ряду, тобто визначаємо наявність в часовому ряді певних компонент.

Перш за все, це вплив на змінну *У ефекту сезонності*. Графік дозволяє встановити наявність цього фактору в явищі, яке вивчається, та визначити природу (або *характер*) такого типу *регулярних коливань*. На практиці виділяють два типи сезонних коливань:

- ✓ *Адитивні*; та
- ✓ *Мультиплікативні*.

Нагадаємо (див. [5]), що йдеться про *сили впливу* сезонних факторів на досліджуване явище, тобто про методи вимірювання *інтенсивності* сезонних коливань у часовому ряді. Поєднуючи «*логічний аналіз*» економічної суті явища, що досліджується, з графічним аналізом графіка часових рядів, який представляє його динаміку, зазвичай виділяють два типи коливань:

- *Адитивні*, або *абсолютні* коливання, які виникають, коли регулярно повторювані сезонні коливання характеризуються *більш-менш постійною різницею* між емпіричними значеннями (y_t) часового ряду і значеннями тренду ($f(t)$ $t = 0, 1, 2, \dots, n$);
- *Мультиплікативні*, або *відносні* коливання, які виникають, коли регулярно повторювані сезонні коливання характеризуються *більш-менш постійним відношенням* емпіричних значень (y_t) часового ряду і значень тренду ($f(t)$ $t = 0, 1, 2, \dots, n$);

У випадку «*мультиплікативного*» *характеру* коливань вплив на змінну *У ефекту сезонності* є *пропорційний тренду*, а «*сила*» цього впливу визначається певним *множником*.

- На графіку ряду легко виявити «нетипові» спостереження.

Візуальний аналіз графіка дуже корисний для визначення «зворотних» моментів для досліджуваного явища:

- Тобто пунктів, де змінюється *напрямок* його розвитку.

Графік часових рядів відіграє дуже важливу роль при побудові *аналітичної моделі тенденції розвитку*:

Форма «смуги», утворена точками графіка, визначає *гіпотетичну форму* моделі, тобто конкретну математичну функцію, що може описувати *основний напрям розвитку* досліджуваного явища.

Ось чому візуальний аналіз графіка часового ряду є *обов'язковим* елементом побудови моделі, незалежно від того «механічні», чи *аналітичні* методи згладжування використовуються.

3. Аналітичне згладжування часового ряду.

Різниця між «механічними» та *аналітичними* методи полягає в тому, що «розмите» формулювання, яке відображає сутність «механічних» методів:

«Проведена від руки між точками графіку часового ряду «плавна лінія», яка розташована «максимально близько до них»»;

у випадку *аналітичних* методів отримує чітке математичне визначення того, що формально означає вислів: «максимально близько до них».

Шукана лінія тренду $f(t)$, $t = 0, 1, 2, \dots, n$ явища, що досліджується, повинна «відповідати» результатам спостережень y_t , $t = 0, 1, 2, \dots, n$, значень часового ряду. Припустимо, що на підставі візуального аналізу форми «смуги», утвореної точками графіка $\{(t, y_t), t = 0, 1, 2, \dots, n\}$ часового ряду, сформульовано гіпотезу щодо *основного напрямку розвитку* досліджуваного явища: описує:

- Лінію тренду визначає функція $f(t) = f(t/\theta_1, \dots, \theta_k)$, яка залежить від параметрів $(\theta_1, \dots, \theta_k)$.

При цьому параметри $(\theta_1, \dots, \theta_k)$, які називаються *структурними* параметрами, невідомі.

- Суть «аналітично-статистичних» методів згладжування часового ряду полягає в тому, щоб знайти такі оцінки $(\hat{\theta}_1, \dots, \hat{\theta}_k)$ параметрів $(\theta_1, \dots, \theta_k)$, для яких функція $f(t/\hat{\theta}_1, \dots, \hat{\theta}_k)$ буде «найкраще відповідати» точкам графіка $\{(t, y_t), t = 0, 1, 2, \dots, n\}$ часового ряду.

Можна запропонувати багато різних критеріїв «найкращої відповідності» функцій конкретним точкам:

- Математична специфікація такого критерію визначає *метод* оцінки структурних параметрів моделі.

З багатьох причин одним із найпопулярніших і найчастіше використовуваних методів, особливо в практиці економетричних досліджень, є метод найменших квадратів (МНК). Він є також базовим інструментом оцінювання параметрів в цій книзі.

Отримані в результаті спостережень значення y_1, y_2, \dots, y_n , називаються *емпіричними значеннями* змінної Y ;

Числа, отримані за формулою:

$$\hat{y}_t = f(t / \hat{\theta}_1, \dots, \hat{\theta}_k), t = 1, 2, \dots, n,$$

називаються *теоретичними значеннями* для відповідних спостережень y_t змінної Y .

Множина всіх теоретичних значень:

$$\{(t, \hat{y}_t), t = 0, 1, 2, \dots, n\}$$

утворює *лінію регресії* змінної Y .

Різниці: $e_t = y_t - \hat{y}_t, t = 1, 2, \dots, n$, між *емпіричними* та *теоретичними значеннями* змінної Y називаються *рештами*.

➤ У випадку *методу найменших квадратів* критерієм того, що лінія: $f(t) = f(t/\theta_1, \dots, \theta_k)$ «найкраще відповідає» статистичній вибірці:

$$f(t/\theta_1, \dots, \theta_k) \Leftrightarrow \{(1, y_1), (2, y_2), \dots, (n, y_n)\}$$

є мінімум суми *квадратів залишків*.

Іншими словами, нехай: $\theta = (\theta_1, \dots, \theta_k), \hat{\theta} = (\hat{\theta}_1, \dots, \hat{\theta}_k)$.

$$S^2(\theta) = \sum_{t=1}^n (y_t - f(t/\theta))^2.$$

Тоді наступна рівність може слугувати строгим визначенням МНК-оцінок:

$$\hat{\theta} = (\hat{\theta}_1, \dots, \hat{\theta}_k)$$

параметрів $\theta = (\theta_1, \dots, \theta_k)$ лінії тренду $f(t) = f(t/\theta_1, \dots, \theta_k)$, на основі статистичної вибірки $\{(1, y_1), (2, y_2), \dots, (n, y_n)\}$:

$$S^2(\hat{\theta}_1, \dots, \hat{\theta}_k) = \min_{(\theta_1, \dots, \theta_k)} S^2(\theta_1, \dots, \theta_k)$$

3. Ковзне середнє.

У загальному випадку, тобто коли *всі можливі компоненти* присутні в часовому ряді, його аналіз може бути досить складним. Пов'язано це з тим, що природа різних компонент є різною. А це в свою чергу вимагає відповідних математичних засобів для їх опису та аналізу. Тому математичний та статистичний аналіз часового ряду зазвичай починається з його

розкладання на окремі складові, оскільки для кожної з них використовуються різні методи дослідження.

Пригадаємо, що:

➤ Процес ідентифікації та виділення окремих компонентів часових рядів називається *декомпозицією* рядів.

Припустимо, що метою дослідження є *виділення тренду*, тобто:

- На основі отриманих значень часового ряду необхідно визначити *загальний напрямок зміни досліджуваного явища* шляхом усунення всіх можливих коливань.

Досить ефективним у цьому випадку є метод, який називається «ковзним середнім», або методом «*середніх рухомих*».

Зараховуємо його до *механічних* методів, оскільки він не потребує застосування будь-яких аналітичних засобів, а зводиться до *трансформації* (чи *перетворення*) елементів часового ряду

$$\{y_0, y_1, y_2, \dots, y_k, \dots, y_T\}$$

за допомогою простих обчислювальних алгоритмів.

➤ *Ковзне середнє* – це середнє арифметичне заданої кількості послідовних значень у часовому ряді.

- Кількість k послідовних періодів, на основі яких обчислюємо середнє арифметичне, називається *сталюю згладжування*.

Зважаючи на кількість періодів, що складають основу для обчислення ковзної середньої (тобто на значення сталої згладжування k) виділяють *звичайну* та *центровану ковзні середні*.

✓ Звичайні *рухомі середні* значення обчислюються з *непарної* кількості послідовних елементів часового ряду, коли k має вигляд:

$$k = 2 \cdot l + 1, l = 1, 2, \dots,$$

де l – довільне певне *натуральне* число.

✓ Якщо стала згладжування k – *парне натуральне* число, що має вигляд:

$$k = 2 \cdot l, l = 1, 2, \dots,$$

ковзне середнє називається *центрованим*.

Вибір типу ковзного середнього та конкретного значення *сталой згладжування* k залежить від того, які коливань потрібно усунути із часового ряду (див. [4], [5]).

4. Тренд на тлі випадкових коливань.

Варто підкреслити, що у часовому ряді не всі його компоненти *обов'язково* повинні бути одночасно присутніми.

Обов'язковою в часових рядах, отриманих в результаті спостережень за реальними явищами, є наявність в них *випадкової компоненти*, тоді як систематичні компоненти досить часто з'являється лише в одній із можливих їх форм.

✓ Процедура усунення із часових рядів випадкових коливань називається їх згладжуванням.

Якщо йдеться про виділення *тренду* шляхом усунення з часового ряду випадкових коливань, то використовуються *звичайні ковзні середні*.

Сформулюємо задачу більш чітко.

- Припустимо, що значення y_t часового ряду, які представляють результати спостережень досліджуваного явища для послідовних моментів часу $t \in \{1, 2, \dots, n\}$, містять дві складові:

$$y_t = f(t) + \varepsilon_t, \quad t = 1, 2, \dots, n.$$

При цьому функція часу $f(t)$ означає тренд, що виступає в цьому ряді та визначає *головний* напрям розвитку досліджуваного явища.

Тренд $f(t)$ спостерігається на тлі випадкових коливань, що присутні в ряді у вигляді доданку ε_t , ($t = 1, 2, \dots, n$).

✓ Якщо зміни $f(t)$, викликані основними причинами, *значно більші*, ніж відхилення ε_t , спричинені побічними факторами, і величина випадкових коливань ε_t не може «*приховати*» цю *тенденцію* – тоді на графіку часового ряду ми побачимо *смугу* у формі функції $f(t)$ і досить тривалі часові проміжки її змін в одному напрямку:

- Рух *вниз*, тобто *ведмежий* тренд, або
 - Рух *вгору*, тобто *бичачий* тренд.
- ✓ У випадку *бічного* тренду коливання, спричинені систематичною складовою ряду $f(t)$, значно *менші* та *повільніші*, ніж непередбачувані зміни ε_t у значенні досліджуваної змінної. Тому графік ряду має наступний вигляд:
- Спостерігаються «*нерегулярні*» коливання значень навколо *більш-менш постійного* рівня.

Якщо ряд має описану вище структуру, тобто містить тільки дві складові:

$$y_t = f(t) + \varepsilon_t, \quad t = 1, 2, \dots, n,$$

і при цьому функція часу $f(t)$ означає тренд, а метою є усунення випадкових коливань ε_t , $t = 1, 2, \dots, n$, із ряду, то в цьому випадку використовуються *непарні* або *звичайні* ковзні середні.

4.6. Згладжування часових рядів.

1. Звичайні ковзні середні.
2. Непарне ковзне середнє: *приклад*.
3. Згладжування часового ряду.
4. Вибір сталої згладжування k .

1. Звичайні ковзні середні.

Припустимо, що в якості сталої згладжування було визначене непарне значення $k = 2l + 1$ (де $l = 1, 2, \dots$, – якесь натуральне число).

Тоді k -елементним ковзним середнім називається число $\bar{y}_i^{(k)}$, яке обчислюється за формулою:

$$\bar{y}_i^{(k)} = \frac{y_{i-l} + y_{i-l+1} + \dots + y_{i-1} + y_i + y_{i+1} + \dots + y_{i+l-1} + \dots + y_{i+l}}{2l + 1}$$

- ✓ Часовий ряд $\{y_1, y_2, y_3, \dots, y_n\}$, що досліджується називається *первинним*,
- ✓ Часовий ряд $\{\bar{y}_t^{(k)}, t = l + 1, l + 2, \dots, n - 1\}$, отриманий в результаті обчислення ковзної середньої, називається *вторинним* рядом.

Встановимо зв'язок між моментами спостережень, тобто послідовними моментами часу $t \in \{1, 2, \dots, n\}$, елементами часового ряду y_t , та елементами $\bar{y}_t^{(k)}$ вторинного ряду.

- Послідовні елементи y_t первинного часового ряду *підпорядковуються* відповідним послідовними моментами часу $t \in \{1, 2, \dots, n\}$:

$$y_t \Leftrightarrow t, t \in \{1, 2, \dots, n\}.$$

- Значення $\bar{y}_t^{(k)}$ *непарної* або *звичайної* ковзної середньої записуються на рівні «середнього» часового моменту серед тих значень первинного часового ряду, на підставі яких його отримано.

Іншими словами, нехай $k = 2l + 1$, а

$$\bar{y}_{s^*}^{(k)} = \frac{y_{s+1} + y_{s+2} + \dots + y_{s+k}}{k}.$$

Тобто значення *звичайної* ковзної середньої $\bar{y}_{s^*}^{(k)}$ обчислено на підставі k наступних послідовних елементів *первинного* часового ряду:

$$y_{s+1}, y_{s+2}, \dots, y_{s+k},$$

що відповідають моментам часу $s + 1, s + 2, \dots, s + k$. Зважаючи на спосіб обчислення $\bar{y}_{s^*}^{(k)}$, це ковзне середнє повинно бути віднесене до моменту:

$$s^* = \frac{(s + 1) + (s + k)}{2}.$$

Якщо припустити, що $k = 2l + 1$, то *перший* період часу ($t_{\min} = s^*_{\min}, s = 0$), для якого буде існувати відповідне значення *вторинного* ряду, дорівнює:

$$s_{min} = \frac{1+k}{2} = \frac{1+2l+1}{2} = l+1.$$

Відповідно останнім ($t_{maz} = s^*_{maz}$, $s+k=n$):

$$s_{maz} = \frac{(n-k+1)+n}{2} = \frac{n-2l-1+1+n}{2} = \frac{2n-2l}{2} = n-l.$$

Тобто перші:

$$l - (t = 1, 2, \dots, l)$$

та останні

$$l - (t = n-l+1, n-l+2, \dots, n)$$

періодів не будуть мати відповідних значень ковзного середнього $\bar{y}_{s^*}^{(k)}$.

Таким чином, для непарного значення $k = 2l + 1$ вторинний ряд має відповідні значення для моментів часу $s^* = l + 1, l + 2, \dots, n - l$:

$$\bar{y}_{l+1}^{(k)}, \bar{y}_{l+2}^{(k)}, \dots, \bar{y}_{n-l}^{(k)},$$

і є коротшим від первинного на $2l = k - 1$ значень.

Проілюструємо це на простому прикладі:

- Припустимо, що маємо часовий ряд

$$\{y_1, y_2, y_3, y_4, y_5, y_6, y_7\},$$

який складається з $n = 7$ елементів.

В якості сталої згладжування виберемо значення: $k = 2l + 1$

$$k = 5 = 2 \cdot 2 + 1; l = 2.$$

Тоді вторинний ряд має вигляд $\{\bar{y}_3^{(5)}, \bar{y}_4^{(5)}, \bar{y}_5^{(5)}\}$, де

$$\bar{y}_3^{(5)} = \frac{y_1 + y_2 + y_3 + y_4 + y_5}{5};$$

$$\bar{y}_4^{(5)} = \frac{y_2 + y_3 + y_4 + y_5 + y_6}{5};$$

$$\bar{y}_5^{(5)} = \frac{y_3 + y_4 + y_5 + y_6 + y_7}{5}.$$

Тобто для періодів ($t = 1$), ($t = 2$) і ($t = 6$), ($t = 7$), немає відповідних ковзних середніх значень $\bar{y}_t^{(5)}$.

2. Непарне ковзне середнє: приклад.

Приклад 1. Наступний часовий ряд відображає попит на певний товар (тис. шт.) протягом року.

$$y_1 = 26; y_2 = 25; y_3 = 31; y_4 = 23; y_5 = 32; y_6 = 31; \\ y_7 = 33; y_8 = 28; y_9 = 31; y_{10} = 33; y_{11} = 25; y_{12} = 27.$$

Припускаючи, що зміни рівня продаж були викликані випадковими чинниками, провести згладжування часового ряду, елімінуючи випадкові вагання. З цією метою використати метод непарних ковзних середніх для наступних сталих згладжування: $k = 3$; $k = 5$; $k = 7$.

Розв'язок: Результати всіх обчислень приведені в таблиці 1.

Непарне ковзне середнє.

Первинний ряд y_t		Вторинний ряд y_t^*		
t	y_t	$y_t^* (k = 3)$	$y_t^* (k = 5)$	$y_t^* (k = 7)$
1	$y_1 = 26$			
2	$y_2 = 25$	$y_2^* = 27,33$		
3	$y_3 = 31$	$y_3^* = 26,33$	$y_3^* = 27,4$	
4	$y_4 = 23$	$y_4^* = 28,66$	$y_4^* = 28,4$	$y_4^* = 28,71$
5	$y_5 = 32$	$y_5^* = 28,66$	$y_5^* = 30,0$	$y_5^* = 29,0$
6	$y_6 = 31$	$y_6^* = 32,0$	$y_6^* = 29,4$	$y_6^* = 29,85$
7	$y_7 = 33$	$y_7^* = 30,66$	$y_7^* = 31,0$	$y_7^* = 30,14$
8	$y_8 = 28$	$y_8^* = 30,66$	$y_8^* = 31,2$	$y_8^* = 30,42$
9	$y_9 = 31$	$y_9^* = 30,66$	$y_9^* = 30,0$	$y_9^* = 29,71$
10	$y_{10} = 33$	$y_{10}^* = 29,66$	$y_{10}^* = 28,8$	
11	$y_{11} = 25$	$y_{11}^* = 28,33$		
12	$y_{12} = 27$			

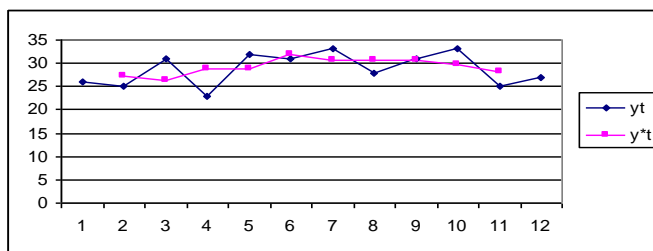
Таблиця 1.

Наведемо для прикладу кілька детальних обчислень елементів вторинного ряду для різних значень сталої згладжування:

1. $k = 3$.

$$y_2^{(3)} = \frac{26 + 25 + 31}{3} = 27,33; y_3^{(3)} = \frac{25 + 31 + 23}{3} = 26,33;$$

$$y_4^{(3)} = \frac{31 + 23 + 32}{3} = 28,66; \text{ ітд.}$$



Мал. 1. 3-елементне ковзне середнє.

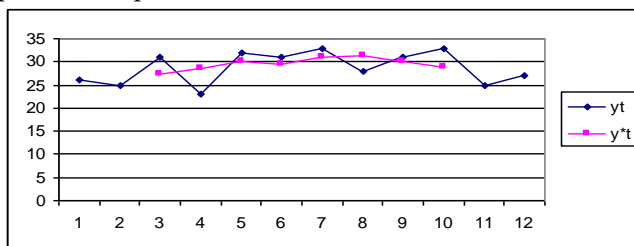
Спільний графік первинного ряду та вторинного ряду для 3-елементного ковзного середнього приведено на мал. 1.

2. $k = 5$.

$$y_3^{(5)} = \frac{26 + 25 + 31 + 23 + 32}{5} = 27,4; y_4^{(5)} = \frac{25 + 31 + 23 + 32 + 31}{5} = 28,4;$$

$$y_{4}^{(5)} = \frac{31+23+32+31+33}{5} = 30,0; \text{ ітд.}$$

Спільний графік первинного ряду та вторинного ряду для 5-елементного ковзного середнього приведено на мал. 2.



Мал. 2. 5-елементне ковзне середнє.

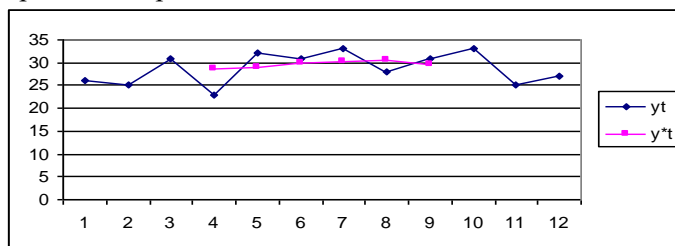
3. $k = 7$.

$$y_{4}^{(7)} = \frac{26+25+31+23+32+31+33}{7} = 28,71;$$

$$y_{5}^{(7)} = \frac{25+31+23+32+31+33+28}{7} = 29,0;$$

$$y_{6}^{(7)} = \frac{31+23+32+31+33+28+31}{7} = 29,85; \text{ ітд.}$$

Спільний графік первинного ряду та вторинного ряду для 7-елементного ковзного середнього приведено на мал. 3.



Мал. 3. 7-елементне ковзне середнє.

3. Згладжування часового ряду.

➤ Використання ковзної середньої до згладжування часового ряду, або інакше – «метод середніх рухомих», полягає у заміні емпіричних даних y_t для послідовних періодів спостережень (первинний ряд) на середнє арифметичне значення явища $\bar{y}_i^{(k)}$ з досліджуваного періоду та декількох суміжних періодів (вторинний ряд).

Згідно з припущенням, значення y_t часового ряду має в своїй структурі тільки дві складові:

$$y_t = f(t) + \varepsilon_t, \quad t = 1, 2, \dots, n.$$

Тобто окрім тенденції розвитку $f(t)$, у досліджуваному ряді є лише випадкові коливання ε_t ,

Використовуючи словосполучення «випадкові коливання», вважаємо, що коливання ε_t , які «присутні» в значенні y_t , не містять постійної, тобто систематичної (позитивної чи негативної) складової.

На практиці це означає:

- ✓ Відхилення від тренду, спричинені випадковими коливаннями ε_t , в різні періоди часу t є різноспрямованими.

І якщо ми трактуємо «випадкове коливання» ε_t як випадкову величину, то це означає, що її математичне сподівання дорівнює нулю:

$$E(\varepsilon_t) = 0.$$

Враховуючи визначення $\bar{y}_i^{(k)}$ отримаємо:

$$\bar{y}_{s^*}^{(k)} = \frac{f(s+1) + f(s+2) + \dots + f(s+k)}{k} + \frac{\varepsilon_{s+1} + \varepsilon_{s+2} + \dots + \varepsilon_{s+k}}{k}.$$

Тобто

$$\bar{y}_{s^*}^{(k)} = \bar{f}_{s^*}^{(k)} + \bar{\varepsilon}_{s^*}^{(k)}, \text{ де: } \bar{\varepsilon}_{s^*}^{(k)} = \frac{\varepsilon_{s+1} + \varepsilon_{s+2} + \dots + \varepsilon_{s+k}}{k}.$$

Беручи до уваги, що відхилення, спричинені випадковими коливаннями в різні періоди часу t є різноспрямованими, тобто доданки ε_{t+i} в чисельнику виразу для $\bar{\varepsilon}_{s^*}^{(k)}$ мають різні знаки, робимо висновок, що при обчисленні середньої арифметичної $\bar{y}_{s^*}^{(k)}$ ці коливання (принаймні частково) компенсують один одного.

Таким чином, при перетворенні:

$$y_t \rightarrow \bar{y}_{s^*}^{(k)}$$

усуваються (принаймні частково) випадкові коливання ε_t :

$$\bar{\varepsilon}_{s^*}^{(k)} \approx 0.$$

Тобто:

$$\bar{y}_{s^*}^{(k)} \approx \bar{f}_{s^*}^{(k)} \approx f(s^*).$$

➤ Метод ковзних середніх базується на тому, що вторинний ряд, обчислений за допомогою методу середніх рухомих, трактується як наближення шуканої лінії тренду $f(t)$.

4. Вибір сталої згладжування k .

Формула для обчислення ковзного середнього $\bar{y}_{s^*}^{(k)}$ пояснює також назву: «механічні методи»:

- ✓ Лінія тренду $f(t)$ отримується без необхідності робити будь-які додаткові припущення щодо її форми, а виключно «механічним чином» – шляхом підрахунку середньої рухомої.

З прийнятих припущень випливає, що чим більша кількість (k) періодів є основою для обчислення ковзної середньої величини $\bar{y}_{s^*}^{(k)}$, тим «повніше» чи «краще» випадкові коливання ε_t усуваються з часового ряду y_t .

✓ Чим більше значення сталої згладжування k , тим краще «згладжується» вторинний ряд по відношенню до первинного.

З іншого боку одночасно з усуненням випадкових коливань, «деформуються» також реальні значення $f(t)$ досліджуваного явища для послідовних моментів часу $t \in \{1, 2, \dots, n\}$, в результаті їх перетворення:

$$f(t) \rightarrow \bar{f}_{s^*}^{(k)}$$

Тому вибір відповідного в конкретній практичній ситуації значення сталої згладжування k є окремим завданням, для розв'язування якого існують як теоретичні, так і емпіричні методи.

На практиці часто використовується експериментальний метод вибору сталої згладжування k шляхом послідовних емпіричних наближень. Він буде детально розглянутий на конкретних числових прикладах.

4.7. «Ковзне середнє» як адаптивний метод прогнозування: приклади та завдання для самоконтролю.

Економетрико-статистичні методи в дослідженні економічних процесів

1. Адаптивні моделі 2. Метод ковзних середніх. 3. Експериментальний метод вибору сталої згладжування k . 4. Метод ковзних середніх: приклад. 5. Процедура «Ковзне середнє» аркушу «Excel».

1. Адаптивні моделі.

Маючи велику кількість позитивних властивостей моделі тенденції розвитку знайшли широке розповсюдження в практичних дослідженнях. Однак використання їх в прогностичних цілях має ряд очевидних недоліків.

- По-перше, спірним є самий базовий принцип економетричного прогнозування, особливо якщо йдеться про економічні явища.

Стосовно моделей тенденції розвитку цей принцип означає стабільність в часі механізму розвитку досліджуваних явищ та незмінність аналітичного вигляду і параметрів функції тренду.

Аналітичні методи усунення випадкових коливань, які використовуються при побудові моделі тенденції розвитку, гарантують отримання «середньо хорошої» моделі, яка «найкраще» відповідає всім значенням часового ряду $\{y_1, y_2, \dots, y_n\}$ прогнозовної змінної, отриманим в результаті спостережень.

Це може бути перевагою моделі на етапі *аналізу* досліджуваного явища, коло йдеться про виявлення притаманних йому закономірностей. Однак при визначенні прогнозу, особливо *короткострокового* прогнозу, дуже важливими можуть бути *останні* спостереження прогнозної змінної. Згладжування даних, виконане в процесі побудови моделі, *нівелює*, (в певному розумінні – *знищує*) корисну для прогнозу інформацію, яку містять в собі останні спостереження.

Для опису в часі явищ, що характеризуються *нерегулярними* змінами напрямку чи швидкості тренду, або викривленням і зсувом періодичних коливань, використовують адаптивні моделі. Ці моделі зазвичай особливо ефективні (див. [підрозділ 4. 3](#)), коли часовий ряд містить дві складові:

- Перша – *випадкові коливання*;
- Друга – *структурна* складова у вигляді «*майже постійного*» (порівняно з випадковими коливаннями) *рівня*.

Іншими словами, коли значення змінної, що спостерігається, «*коливаються*» навколо більш-менш постійного рівня.

Адаптивні моделі побудовані таким чином, щоб врахувати можливість *нестабільності* економічної структури та *можливості зміни* параметрів моделі у часі.

- Адаптивні моделі не містять апріорної сталості аналітичної форми функції тренду або параметрів, що зустрічаються в ній, в усьому проміжку дослідження.

Це забезпечує високу гнучкість цих моделей, що робить їх зручним і дешевим інструментом для побудови короткострокових прогнозів. Множина методів прогнозування побудованих на основі адаптивних моделей дуже широка. Розглянемо кілька найпростіших та найпопулярніших серед них.

2. Метод ковзних середніх.

Припустимо, що маємо часовий ряд $\{y_1, y_2, \dots, y_n\}$ прогнозованої змінної Y в інтервалі часу $t = 1, 2, \dots, n$.

Стала згладжування визначена і дорівнює k .

- Тоді *точковий прогноз* y_{n+1}^* цієї змінної на момент часу $(n + 1)$, визначений методом *ковзної середньої*, буде дорівнювати середньому арифметичному з останніх k спостережень $(y_{n-k+1}, \dots, y_{n-1}, y_n)$ часового ряду прогнозної змінної:

$$y_{n+1}^* = \frac{y_{n-k+1} + y_{n-k+2} + \dots + y_n}{k} = \frac{1}{k} \sum_{i=0}^{k-1} y_{n-i}.$$

- ✓ З одного боку, чим *менша* стала згладжування k , тим *меншим* буде ефект згладжування часового ряду, і, як наслідок, тим *більший* вплив на точковий прогноз y_{n+1}^* матимуть присутні в часовому ряді випадкові коливання.
 - В той же час, однак, середнє арифметичне, визначене з *меншої* кількості спостережень, *швидше* відобразатиме *поточні* зміни значень прогнозованого явища.
- ✓ З іншого боку, ковзне середнє значення, яке визначається з *більшої* кількості спостережень, *краще згладить* ряд.
 - В наслідок цього точковий прогноз y_{n+1}^* *повільніше* реагуватиме на *зміни рівня* прогнозованої змінної Y .

Тому вибір константи згладжування k повинен бути *компромісом* між цими можливостями. Константу k визначає дослідник, і його рішення щодо цього вибору, перш за все, повинно ґрунтуватися на здобутому у минулому досвіді.

Однак найчастіше параметр k визначається методом *послідовних емпіричних наближень* експериментальним способом. Для цього, наприклад, можуть бути використані помилки *ex-post* за минулі періоди (див. підрозділ 2. 1).

Якщо стала згладжування дорівнює k , то згідно з визначенням перший *точковий прогноз* (y_{k+1}^*) можна визначити на момент часу $(k + 1)$:

$$y_{k+1}^* = \frac{y_1 + y_2 + \dots + y_k}{k} = \frac{1}{k} \sum_{i=1}^k y_i .$$

Це означає, що для наступних значень $[y_{k+1}, y_{k+2}, \dots, y_n]$ часового ряду $\{y_1, y_2, \dots, y_n\}$, будуть визначені відповідні точкові прогнози *ex post*:

$$[y_{k+1}^*, y_{k+2}^*, \dots, y_n^*].$$

- Таким чином, інтервал часу $t = k + 1, k + 2, \dots, n$, що містить $(n - k)$ періодів, можна трактувати як *інтервал емпіричної верифікації прогнозів*, отриманих методом *ковзних середніх* з постійною згладжування k .

3. Експериментальний метод вибору сталої згладжування k .

У випадку вибору сталої згладжування k згаданий вище експериментальний метод послідовних емпіричних наближень виглядає наступним чином:

- ✓ Визначається відповідна до ситуації, що розглядається, міра «*точності прогнозу*», та вибирається показник помилки прогнозу *ex post*.
- ✓ Визначається набір $K = [k_1, k_2, \dots, k_s]$ можливих значень, найбільш «*нідходящих*» для ролі сталої згладжування у розглянутій ситуації.
- ✓ Для всіх значень $k \in K$ визначаються прогнози *ex post*:

$$[y_{k+1}^*, y_{k+2}^*, \dots, y_n^*].$$

- ✓ Для всіх значень $k \in K$ обчислюються значення вибраного показника помилки прогнозу *ex post* в інтервал емпіричної верифікації прогнозів.
- ✓ Остаточо серед можливих значень $K = [k_1, k_2, \dots, k_s]$ вибирається така стала згладжування, для якої прогноз *ex post* є «найбільш точним» згідно з обраним критерієм.

Як показали відповідні дослідження, метод ковзних середніх є одним з найпопулярніших методів прогнозування. Це обумовлено наступними його властивостями:

- *Він швидкий, простий у використанні, дешевий; а головне:*
- *Не потребує при його застосуванні спеціальних знань з області статистичної теорії прогнозу.*

Крім цих очевидних переваг, він має також суттєві *недоліки*.

- ✓ Перш за все, при побудові прогнозу y_{n+1}^* не враховуються всі спостереження часового ряду $\{y_1, y_2, \dots, y_n\}$, а лише останні k спостережень:

$$(y_{n-k+1}, \dots, y_{n-1}, y_n).$$

- ✓ Не виконується один з основних *евристичних принципів* теорії прогнозів – «*постулат старіння інформації*».
 - Згідно з цим постулатом: «*новіші дані містять новішу інформацію про прогнозоване явище.*».

Тому визначаючи прогноз *останнім* спостереженням змінної прогнозування Y слід надати порівняно *більшу вагу*, ніж тим, що були *раніше*.

- ✓ При використанні ж методу ковзної середньої *всім значенням* прогнозованої змінної у формулі, на основі якої визначається прогноз y_{n+1}^* , надаються *однакові ваги* величиною $(1/k)$.

4. Метод ковзних середніх: приклад.

В попередньому підрозділі 4. 6 було розглянуто приклад згладжування часового ряду, елімінуючи випадкові вагання за допомогою *методу непарних ковзних середніх*. В якості *сталих згладжування* використовувались числа: $k = 3$; $k = 5$; $k = 7$. Варто при цьому зауважити, що алгоритм отримання згладженого значення $\bar{y}_i^{(k)}$ *вторинного* ряду, коли йдеться виключно про «*усунення*» із часового ряду випадкових коливань, суттєво відрізняється, від алгоритму визначення чергових значень (y_{k+i}^*) *точкового прогнозу* методом «*рухомої середньої*» (або «*ковзної середньої*»).

Метод «*ковзної середньої*» зараховується до множини *адаптивних* методів, і зазвичай використовується для *короткострокового оперативного прогнозування* у випадку, якщо в досліджуваному *одновимірному*

часовому ряді $\{y_1, y_2, y_3, \dots, y_n\}$ немає *систематичної* складової (тобто *тренду*), а також немає періодичної (або *сезонної*) складової.

Обчислювальні алгоритми адаптивних методів передбачають автоматичне згладжування часового ряду. Тому *стала згладжування* є одним із обов'язкових їх параметрів.

- В методі «ковзної середньої», що розглядається, таким параметром (тобто сталою згладжування) є натуральне число k , яке визначає кількість елементів часового ряду, що бере участь у середній рухомій.

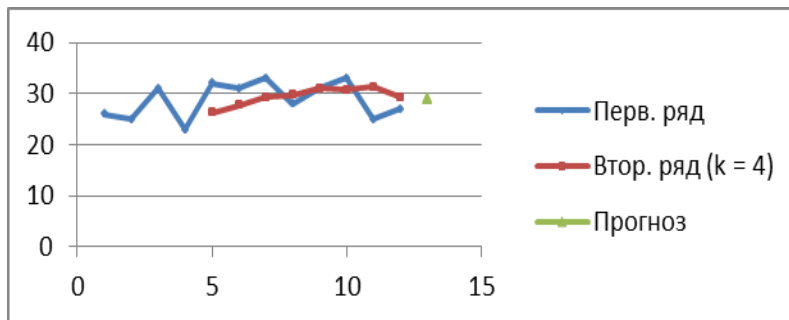
Приклад. Наступний часовий ряд відображає попит на певний товар (*тис. шт.*) протягом року.

$$y_1 = 26; y_2 = 25; y_3 = 31; y_4 = 23; y_5 = 32; y_6 = 31; \\ y_7 = 33; y_8 = 28; y_9 = 31; y_{10} = 33; y_{11} = 25; y_{12} = 27.$$

На підставі цього ряду необхідно виконати *оперативне прогнозування* можливого чергового значення цього часового ряду.

Тобто необхідно обчислити *короткостроковий прогноз* $\{y^*_{13}\}$ попиту на цей товар в наступному місяці.

Розв'язок: 1) Використовуючи графік часового ряду провести *вступну* (попередню) *ідентифікацію* ряду і переконатись, що в ньому відсутні *систематична* складова (тобто *тренд*), а також немає періодичної складової.



2) Для обчислення короткострокового прогнозу $\{y^*_{13}\}$ попиту в наступному місяці скористатися методом «*рухомої середньої*».

3). Використовуючи експериментальний метод вибрати сталу згладжування k . З цією метою:

3(а). Визначити наступний набір $K = [2, 3, 4]$ можливих значень для ролі сталої згладжування k .

3(б). Встановити критерій для вибору сталої згладжування k серед можливих її значень з множини $K = [2, 3, 4]$.

➤ В якості остаточного критерію для вибору сталої згладжування k серед можливих її значень з множини K застосувати синтетичний показник:

$$\Sigma = MAE + S + U^M, \text{ де } S = \sqrt{S^2} = \sqrt{MSE}$$

• *Найбільш точним* будемо вважати прогноз *ex post* для того $k \in K$, для якого сума, що вибрана в якості критерію, є *мінімальною*.

3(в). Для всіх значень $k = 2, 3, 4$, визначаються прогнози *ex post*

$$[y_{k+1}^*, y_{k+2}^*, \dots, y_n^*].$$

В даному випадку таким прогнозом будуть *k-елементні ковзні середні*

обчислені за формулою: $y_{t+1}^* = \frac{y_t + y_{t-1} + \dots + y_{t-k+1}}{k}$, $t = n, n-1, \dots, k$.

3(г). Для всіх значень $k = 2, 3, 4$, обчислити наступні показники помилки прогнозу *ex post* в інтервал емпіричної верифікації:

1. *Середню безумовну абсолютну похибку* прогнозу *ex-post*:

$$MAE = \frac{1}{n-k} \cdot \sum_{t=k+1}^n |y_t - y_t^*|.$$

Відповідь: $MAE_{(k=2)} = 3,75$; $MAE_{(k=3)} = 3,519$; $MAE_{(k=4)} = 3,156$.

2. *Середньо-квадратичну помилку* прогнозу *ex-post* :

$$S^2 = MSE = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t - y_t^*)^2.$$

Відповідь: $MSE_{(k=2)} = 17,625$; $MSE_{(k=3)} = 15,099$; $MSE_{(k=4)} = 13,742$.

$S_{(k=2)} = 4,198$; $S_{(k=3)} = 3,886$; $S_{(k=4)} = 3,707$.

3. Коефіцієнт *зміщення прогнозу*: $U^M = \frac{(\bar{y} - \bar{y}^*)^2}{MSE}$,

$$\text{де } \bar{y} = \frac{1}{n-k} \cdot \sum_{t=k+1}^n y_t \text{ та } \bar{y}^* = \frac{1}{n-k} \cdot \sum_{t=k+1}^n y_t^*.$$

Відповідь: $U^M_{(k=2)} = 0,0013$; $U^M_{(k=3)} = 0,002$; $U^M_{(k=4)} = 0,026$.

4. Коефіцієнт *змінності прогнозу*:

$$U^S = \frac{(\sigma_y - \sigma_{y^*})^2}{MSE}; \text{ де } \sigma_y = \sqrt{\sigma_y^2} \text{ та } \sigma_{y^*} = \sqrt{\sigma_{y^*}^2},$$

$$\text{а } \sigma_y^2 = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t - \bar{y})^2; \text{ та } \sigma_{y^*}^2 = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t^* - \bar{y}^*)^2$$

Відповідь: $U^S_{(k=2)} = 0,076$; $U^S_{(k=3)} = 0,194$; $U^S_{(k=4)} = 0,101$.

4) Для всіх значень $k \in K$ знайти величину синтетичного показника Σ .

Відповідь: $\Sigma_{k=2} = 7,9494$; $\Sigma_{k=3} = 7,4065$; $\Sigma_{k=4} = 6,8889$. $\min(\Sigma_k) = 6,8889$; $k = 4$.

5) Обчислити *короткостроковий прогноз* $\{y_{13}^*\}$ попиту на досліджуваний товар в наступному місяці. **Відповідь:** $y_{13}^* = 30,6$.

6. Процедура «Ковзне середнє» аркушу «Ехсел».

Застосовуючи процедуру «Ковзне середнє» програми «Аналіз даних» модуля «Дані» аркушу «Ехсел» і використовуючи часовий ряд y_1, y_2, \dots, y_n обчислити короткостроковий прогноз $\{y_{n+1}^*\}$ попиту в наступному місяці для різних значень сталої згладжування k з множини $K = [2, 3, 4]$.

4.8. Метод експоненціального згладжування.

1. Метод експоненціального згладжування. 2. Алгоритм методу експоненціального згладжування. 3. Метод експоненціального згладжування. (Приклад).

1. Метод експоненціального згладжування.

Цей метод повною мірою відображає назву – «*адаптивні методи*» і може бути використаний для ілюстрації *суті* методів, що розглядаються. Принципи, реалізовані в методі *експоненціального згладжування*, переконливо відображають зміст поняття «*адаптація*», тобто «*притосування до існуючої ситуації*».

В цьому методі усунення випадкових коливань із спостережень часового ряду здійснюється механічним шляхом – за допомогою обчислення *середнього значення* заданого часового ряду. Але на відміну від *звичайного середнього* арифметичного, коли всі члени ряду трактуються однаково, обчислюється *зважена середня*, коли останнім спостереженням даються *більші ваги*, а попереднім – менші.

- Таким чином, експоненціальний метод реалізує постулат *старіння інформації* та використовує *всю наявну інформацію* для визначення прогнозу, а отже позбавлений вад *методу ковзних середніх*.

Суттєвим чином цей метод відрізняється від попереднього також *способом* отримання прогнозованого значення:

- Новий прогноз формується в результаті *адаптації*, тобто притосування до *реальних спостережень* попереднього прогнозу.

Корекція попереднього прогнозу базується на врахуванні його *точності* і відбувається шляхом *дослідження похибки*, яка існує в даний момент.

Пояснимо це детальніше. Прогностична процедура має *послідовний* характер.

- ✓ Припустимо, що відоме значення y_t^* прогнозу досліджуваної змінної в момент часу t .

Якщо припустити, що маємо також можливість виміряти *фактичне значення* y_t прогнозованої змінної в цей момент часу, то можна обчислити помилку *ex post*:

$$e_t = y_t - y_t^*.$$

- Якщо прогноз y_t^* на період t був «*занижений*» порівняно з фактичним значенням змінної прогнозу y_t , то прогноз y_{t+1}^* на період $(t + 1)$ *збільшиться* порівняно з попереднім прогнозом y_t^* .

- І навпаки, якщо прогноз y_t^* на період t був «завищений» в порівнянні фактичним значенням змінної прогнозу y_t , то прогноз y_{t+1}^* на період $(t + 1)$ слід зменшити в порівнянні з попереднім прогнозом y_t^* .

Помилка прогнозу *ex post* e_t оцінює його *точність* та вказує на те, чи був він «занижений» (у випадку, якщо $e_t < 0$ від'ємна), чи навпаки – «завищений» (у випадку, якщо $e_t > 0$ додатна).

- Метод експоненціального згладжування полягає в тому, щоб *коригувати* величину (y_t^*) попереднього прогнозу, спираючись на цю інформацію.

Додаючи до попереднього прогнозу y_t^* «певну частину» (α) обчисленої помилки прогнозу *ex post* e_t , зважаючи на її знак досягаємо поставленої мети.

Залишається відкритим питання:

- Якою *конкретно* повинна бути ця «певна частина α »?
- Подібно, як і в методі «ковзної середньої» параметр α називається *сталю згладжування*, з тією однак різницею, що цьому випадку:

$$0 < \alpha < 1,$$

тобто α – це якесь число з інтервалу $(0, 1)$.

2. Алгоритм методу експоненціального згладжування.

Використовуючи введені вище позначення, описану процедуру корегування прогнозу y_{t+1}^* можна записати наступною формулою:

$$y_{t+1}^* = y_t^* + \alpha \cdot e_t = y_t^* + \alpha \cdot (y_t - y_t^*), t = 1, 2, \dots$$

Або еквівалентним чином:

$$y_{t+1}^* = \alpha \cdot y_t + (1 - \alpha) \cdot y_t^*.$$

Припустимо, що ця процедура застосовується послідовно, крок по кроку, після отримання чергових спостережень:

$$y_1, y_2, \dots, y_t, t = 1, 2, \dots$$

часового ряду. Оскільки стала згладжування α не залежить від часу, то для довільного моменту часу t , та прогнозів (y_t^*), і (y_{t-1}^*) має місце наступне співвідношення:

$$y_t^* = \alpha \cdot y_{t-1} + (1 - \alpha) \cdot y_{t-1}^*, t = 1, 2, \dots$$

Продовжуючи цю рекурентну процедуру отримаємо:

$$\begin{aligned} y_{t+1}^* &= \alpha \cdot y_t + (1 - \alpha) \cdot (\alpha \cdot y_{t-1} + (1 - \alpha) \cdot y_{t-1}^*) = \\ &= \alpha \cdot y_t + \alpha \cdot (1 - \alpha) \cdot y_{t-1} + (1 - \alpha)^2 \cdot y_{t-1}^*. \end{aligned}$$

Або:

$$y_{t+1}^* = \alpha y_t + \alpha(1-\alpha)y_{t-1} + \alpha(1-\alpha)^2 y_{t-2} + \alpha(1-\alpha)^3 y_{t-3} + \dots \\ \dots + \alpha(1-\alpha)^{t-1} y_1 + (1-\alpha)^t y_1^*.$$

Таким чином, усі відомі в момент визначення прогнозу на період $(t+1)$, значення часового ряду y_1, y_2, \dots, y_t , беруть участь у обчисленні величини прогнозу y_{t+1}^* . При цьому послідовним значенням:

$$y_1, y_2, \dots, y_t,$$

присвоюються ваги відповідно:

$$\alpha(1-\alpha)^{t-1}, \alpha(1-\alpha)^{t-2}, \dots, \alpha.$$

Оскільки $0 < \alpha < 1$, то ці ваги зменшуються з «експоненціальною» швидкістю, реалізуючи тим самим на практиці принцип «старіння інформації».

- Звідси походить назва «метод експоненціального згладжування».

Неважко перевірити, що для будь-якого числа $0 < \alpha < 1$, і для будь-якого t виконується рівність:

$$\alpha + \alpha(1-\alpha) + \alpha(1-\alpha)^2 + \alpha(1-\alpha)^3 + \dots + \alpha(1-\alpha)^{t-1} + (1-\alpha)^t = 1.$$

Таким чином, прогноз y_{t+1}^* на період $(t+1)$ – це *середньозважене* значення спостережень y_1, y_2, \dots, y_t та y_1^* .

Описаний алгоритм не дає можливості обчислити значення прогнозу y_1^* на період $(t=1)$. Тому для завершення побудови прогностичної моделі слід визначити його *окремо*

- Якщо маємо часовий ряд y_1, y_2, \dots, y_n , то зазвичай значення прогнозу y_1^* визначається як середнє арифметичне *фрагменту* цього ряду, тобто:

$$y_1^* = \frac{1}{k} \sum_{t=1}^k y_t, \text{ де } 1 \leq k \leq n.$$

Приймаючи до уваги формулу для обчислення прогнозу y_{t+1}^* , варто зауважити, що значення y_1^* «майже не впливає» на значення прогнозу y_{t+1}^* для досить віддалених періодів t :

- В цій формулі y_1^* присутнє з «вагою» $(1-\alpha)^t \approx 0$, оскільки $0 < \alpha < 1$.

При цьому вплив сталої згладжування α на величину прогнозів (y_{t+1}^*) є «дуже відчутним».

Зазвичай значення (α) сталої згладжування заздалегідь невідоме. Зрозуміло, що на його вибір суттєво впливає характер *динаміки* часового ряду y_1, y_2, \dots, y_n , тому в кожному конкретному випадку застосування методу його необхідно визначати *окремо*.

Подібно як і в методі «ковзної середньої», його визначення може бути проведене *експериментальним* шляхом, а саме:

- Визначається відповідна до ситуації *міра точності прогнозу*, та вибирається *показник помилки прогнозу ex post*;
- На основі значень $[y_1, y_2, \dots, y_n]$ часового ряду, для *різних значень* параметра α з інтервалу $(0, 1)$ визначаємо прогнози *ex post* $[y^*_1, y^*_2, \dots, y^*_n]$;
- Остаточно вибирається *така стала згладжування α* , для якої прогноз *ex post ϵ* «найбільш точним» згідно з обраним критерієм.

3. Метод експоненціального згладжування. (Приклад).

Наступний часовий ряд відображає попит на певний товар (*тис. шт.*) протягом року.

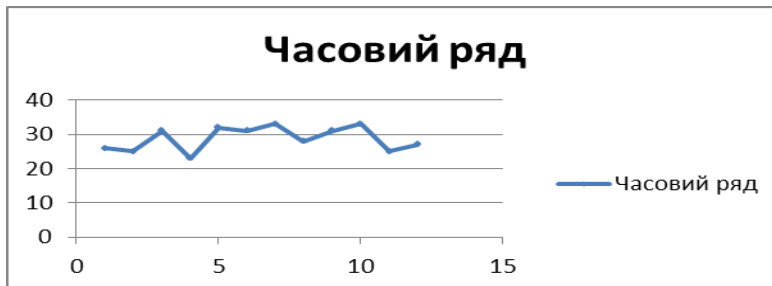
$$y_1 = 26; y_2 = 25; y_3 = 31; y_4 = 23; y_5 = 32; y_6 = 31;$$

$$y_7 = 33; y_8 = 28; y_9 = 31; y_{10} = 33; y_{11} = 25; y_{12} = 27.$$

На підставі цього ряду необхідно виконати *оперативне прогнозування* можливого чергового значення цього часового ряду.

Тобто обчислити *короткостроковий прогноз $\{y^*_{13}\}$* попиту на цей товар в наступному місяці.

Розв'язок: 1) Використовуючи графік часового ряду провести *вступну* (попередню) *ідентифікацію* ряду і переконатись, що в ньому відсутні *систематична* складова (тобто *тренд*), а також немає *періодичної* складової.



2) Для обчислення короткострокового прогнозу $\{y^*_{13}\}$ попиту в наступному місяці скористатися «методом експоненціального згладжування».

3. Використовуючи експериментальний метод вибрати сталу згладжування α . З цією метою:

3(а). Визначити наступний набір:

$$A = [0,1; 0,2; 0,3; 0,4; 0,5; 0,6; 0,7; 0,8; 0,9]$$

можливих значень для ролі *сталого згладжування α* .

3(б). Встановити критерій для вибору сталого згладжування α серед можливих її значень з множини $A = [0,1; 0,2; 0,3; 0,4; 0,5; 0,6; 0,7; 0,8; 0,9]$.

➤ В якості остаточного критерію для вибору сталої згладжування α серед можливих її значень з множини A застосувати синтетичний показник:

$$\Sigma = MAE + S + U^M, \text{ де } S = \sqrt{S^2} = \sqrt{MSE}$$

- Найбільш точним будемо вважати прогноз *ex post* для того $\alpha \in A$, для якого сума, що вибрана в якості критерію, є мінімальною.

3(б). Для всіх значень $\alpha \in A$, визначаються прогнози *ex post*

$$[y^*_1, y^*_2, \dots, y^*_n].$$

В даному випадку прогнозовані значення $\{y^*_t, t = 1, 2, \dots, n\}$ обчислюються наступним чином:

- Процедура прогнозування має *послідовний* характер.
- Оскільки прогноз y^*_1 на період $t = 1$ неможливо обчислити, його значення визначити, як середнє арифметичне *всього* часового ряду:

$$y^*_1 = \frac{1}{n} \cdot \sum_{t=1}^n y_t, (n = 12).$$

- Припустимо, що відоме значення y^*_t прогнозу досліджуваної змінної в момент часу t . Алгоритм визначення прогнозу y^*_{t+1} можна записати наступною формулою:

$$y^*_{t+1} = \alpha \cdot y_t + (1 - \alpha) \cdot y^*_t, t = 1, 2, \dots, n.$$

3(г). Для всіх значень $\alpha \in A$ обчислити наступні показники помилки прогнозу *ex post* в інтервал емпіричної верифікації:

1. Середню безумовну абсолютну похибку прогнозу *ex-post*:

$$MAE = \frac{1}{n-k} \cdot \sum_{t=k+1}^n |y_t - y^*_t|.$$

Відповідь: $MAE_{(\alpha=0,1)} = 3,278$; $MAE_{(\alpha=0,5)} = 3,523$; $MAE_{(\alpha=0,8)} = 3,684$.

2. Середньо-квадратичну помилку прогнозу *ex-post* :

$$S^2 = MSE = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t - y^*_t)^2.$$

Відповідь: $MSE_{(\alpha=0,1)} = 12,194$; $MSE_{(\alpha=0,5)} = 15,577$; $MSE_{(\alpha=0,8)} = 20,018$.

$S_{(\alpha=0,1)} = 3,492$; $S_{(\alpha=0,5)} = 3,467$; $S_{(\alpha=0,8)} = 4,474$.

3. Коефіцієнт зміщення прогнозу: $U^M = \frac{(\bar{y} - \bar{y}^*)^2}{MSE}$,

$$\text{де } \bar{y} = \frac{1}{n-k} \cdot \sum_{t=k+1}^n y_t \text{ та } \bar{y}^* = \frac{1}{n-k} \cdot \sum_{t=k+1}^n y^*_t.$$

Відповідь: $U^M_{(\alpha=0,1)} = 0,0005$; $U^M_{(\alpha=0,5)} = 0,002$; $U^M_{(\alpha=0,8)} = 0,0019$.

4. Коефіцієнт змінності прогнозу:

$$U^S = \frac{(\sigma_y - \sigma_{y^*})^2}{MSE}; \text{ де } \sigma_y = \sqrt{\sigma_y^2} \text{ та } \sigma_{y^*} = \sqrt{\sigma_{y^*}^2},$$

$$\text{а } \sigma_y^2 = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t - \bar{y})^2; \text{ та } \sigma_{y^*}^2 = \frac{1}{n-k} \cdot \sum_{t=k+1}^n (y_t^* - \bar{y}^*)^2$$

Відповідь: $U^S_{(\alpha=0,1)} = 0,689$; $U^S_{(\alpha=0,5)} = 0,157$; $U^S_{(\alpha=0,8)} = 0,027$.

4) Для всіх значень $\alpha \in A$ знайти величину синтетичного показника Σ .

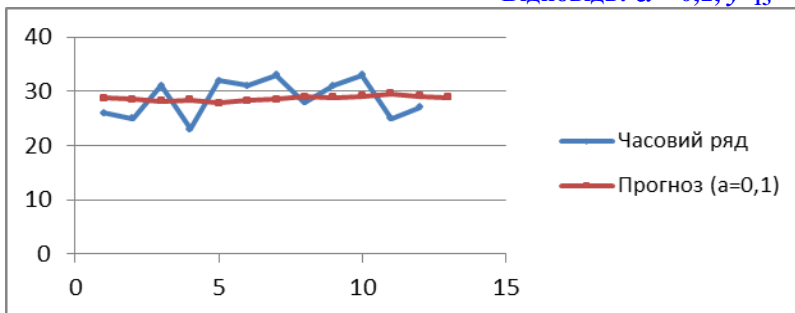
Відповідь: $\Sigma_{(\alpha=0,1)} = 6,7704$; $\Sigma_{(\alpha=0,5)} = 7,4724$; $\Sigma_{(\alpha=0,8)} = 8,1596$.

Використовуючи функцію «ЕСЛИ» аркушу *Excel* визначити значення α сталої згладжування. Сталою згладжування при застосуванні методу рухомої середньої в даному прикладі буде k , для якого Σ_k є мінімальною

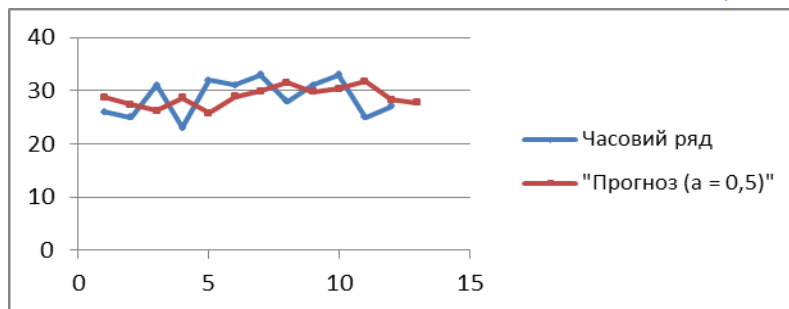
Відповідь: $\min(\Sigma_\alpha) = 6,7704$; $\alpha = 0,1$.

5) Обчислити короткостроковий прогноз $\{y^*_{13}\}$ попиту на досліджуваний товар в наступному місяці.

Відповідь: $\alpha = 0,1$; $y^*_{13} = 28,845$.



Відповідь: $\alpha = 0,5$; $y^*_{13} = 27,671$.



4. Процедура «Експоненціальне згладжування» аркушу «Excel».

Застосовуючи процедуру «Експоненціальне згладжування» програми «Аналіз даних» модуля «Дані» аркушу «Excel» і використовуючи часовий ряд y_1, y_2, \dots, y_n обчислити короткостроковий прогноз $\{y^*_{n+1}\}$ попиту в наступному місяці для різних значень сталої згладжування α з множини A .

4.9. Метод «повзучого тренду».

1. Повзучий тренд з постійним сегментом згладжування. 2. Визначення згладжених значень. 3. Гармонічні ваги. 4. Точковий прогноз, що спирається на «гармонічні ваги». 5. Прогноз на базі «експоненціального згладжування».

1. Повзучий тренд з постійним сегментом згладжування.

Характерною особливістю розглянутих адаптивних методів було те, що дві фази процесу прогнозування були *поєднані*:

✓ *Діагностування минулого* (тобто згладжування емпіричних даних у випадку адаптивних моделей) та *визначення майбутнього* (тобто обчислення прогнозного значення для досліджуваної змінної) відбувалося *одночасно*, в результаті застосування механічних методів усунення випадкових коливань.

Представимо один із методів, в якому ці фази відокремлюються, а з метою «*вирівнювання*» часових рядів застосовується більш складна процедура.

➤ Процес згладжування даних поєднує в собі як *аналітичні*, так і *механічні* засоби усунення випадкових коливань.

Це дає підстави очікувати, що якість згладжування, а отже і якість отриманих прогнозів буде кращою.

Припустимо, що є часовий ряд

$$y_1, y_2, \dots, y_n,$$

який характеризується *нерегулярними коливаннями* змінної прогнозування Y навколо більш-менш постійного рівня, не виявляючи при цьому *чіткої тенденції*.

Сталою згладжування методу, який буде розглядатися, є натуральне число k . В даному випадку його можна пояснити наступним чином:

➤ Хоча розглянутий часовий ряд y_1, y_2, \dots, y_n не демонструє *чіткої тенденції розвитку* протягом *усього періоду* спостереження $[1, 2, \dots, n]$, однак можна припустити, що для менших *під-періодів*, що містять k спостережень ($1 < k < n$), динаміка змінної прогнозування Y має *лінійний* характер.

Тому на *першому кроці* згладжування часового ряду, для всіх послідовних його фрагментів фіксованої довжини k , з метою «*видалення*» випадкових коливання, оцінюються необхідні параметри та будуються лінійні функції тренду.

- Ця особливість методу визначає його назву – «*повзучий тренд з постійним сегментом згладжування*».

Більш конкретно це виглядає наступним чином.

➤ Нехай k означає вибрану для заданого часового ряду сталу згладжування ($k < n$).

- Ділимо часовий ряд: $\{y_1, y_2, \dots, y_n\}$ на послідовні відрізки довжини k :

$$(y_1, y_2, \dots, y_k); (y_2, y_3, \dots, y_{k+1}); \dots; (y_{n-k+1}, y_{n-k+2}, \dots, y_n).$$

Варто зауважити, що принцип «повзучого тренду» створює ситуацію, коли деякі значення y_i часового ряду можуть бути присутніми одночасно в кількох сегментах згладжування.

- Для кожного з цих відрізків, будуємо функції лінійних трендів.

Нехай це будуть функції:

$$f_1(t) = b_1 + a_1 t, t = 1, 2, \dots, k;$$

$$f_2(t) = b_2 + a_2 t, t = 2, 3, \dots, k + 1;$$

...

$$f_{n-k+1}(t) = b_{n-k+1} + a_{n-k+1} t,$$

$$t = n - k + 1, n - k + 2, \dots, n.$$

Оцінювання параметрів $\{(b_i, a_i), i = 1, 2, \dots, n - k + 1\}$, функцій

$$\{f_i(t) = b_i + a_i t, t = i, i + 1, \dots, k + i - 1\}, i = 1, 2, \dots, n - k + 1\},$$

проводиться методом найменших квадратів.

- Згладжуємо кожен з $(n - k + 1)$ послідовних відрізків часового ряду.

З цією метою використовуємо побудовані лінійні тренди та обчислюємо відповідні теоретичні значення:

$$(\hat{y}_1^{(1)} = f_1(1), \hat{y}_2^{(1)} = f_1(2), \dots, \hat{y}_k^{(1)} = f_1(k));$$

$$(\hat{y}_2^{(2)} = f_2(2), \hat{y}_3^{(2)} = f_2(3), \dots, \hat{y}_{k+1}^{(2)} = f_2(k + 1));$$

...

$$(\hat{y}_{n-k+1}^{(n-k+1)} = f_{n-k+1}(n - k + 1), \hat{y}_{n-k+2}^{(n-k+1)} = f_{n-k+1}(n - k + 2) \dots \hat{y}_n^{(n-k+1)} = f_{n-k+1}(n)).$$

2. Визначення згладжених значень.

В результаті цих обчислень для окремих спостережень (y_i) часового ряду $\{y_1, y_2, \dots, y_n\}$, багато з яких можуть бути присутніми одночасно в різних відрізках, отримаємо для того самого моменту часу t декілька різних теоретичних значень на основі різних функцій $f_i(t)$:

Наприклад:

- ✓ Для значень y_1 та y_n буде лише по одному теоретичному значенні, відповідно:

$$\hat{y}_1^{(1)} \text{ та } \hat{y}_n^{(n-k+1)}.$$

- ✓ Для значень y_2 та y_{n-1} – відповідно по два теоретичних значення:

$$\{\hat{y}_2^{(1)}, \hat{y}_2^{(2)}\} \text{ та } \{\hat{y}_{n-1}^{(n-k)}, \hat{y}_{n-1}^{(n-k+1)}\},$$

тощо.

Тому «остаточне» згладжене значення (y_t^*) для спостереження (y_t) часового ряду за період t , буде обчислене на основі всіх таких теоретичних значень, що відповідають y_t середнє арифметичне.

Враховуючи наведені раніше співвідношення, для визначення (остаточно) згладжених значень (y_t^*) можна привести наступну формулу:

$$y_t^* = \frac{1}{1 + g(t) - d(t)} \sum_{j=d(t)}^{g(t)} f_j(t), \quad t = 1, 2, \dots, n,$$

де

$$d(t) = \begin{cases} 1, & \text{для } t = 1, 2, \dots, k \\ t - k + 1, & \text{для } t = k + 1, \dots, n \end{cases},$$

$$g(t) = \begin{cases} t, & \text{для } t = 1, 2, \dots, n - k + 1 \\ n - k + 1, & \text{для } t = n - k + 2, \dots, n \end{cases}.$$

Якщо тепер побудувати графік точок:

$$\{(1, y_1^*), (2, y_2^*), \dots, (n, y_n^*)\},$$

в системі координат $ТОУ$, а потім з'єднати отримані точки послідовно відрізками, отримаємо ломану лінію, що представляє *тенденцію розвитку* часового ряду $\{y_1, y_2, \dots, y_n\}$, який був «згладжений» за допомогою методу *повзучого тренду*.

Варто зауважити, що припущення, згідно з яким часовий ряд:

$$\{y_1, y_2, \dots, y_n\},$$

«не виявляє чіткої тенденції», зовсім не означає, що значення змінної прогнозування Y є незмінним (тобто вона зберігає *постійне* значення) в інтервалі спостереження.

Воно означає лише те, що:

- ✓ Коливання, викликані *систематичною складовою ряду*, значно *менші* та *повільніші*, ніж викликані *непередбачуваними чинниками*, коливання *випадкової складової*, яка впливає на значення досліджуваної змінної.

Тому з точки зору *мети прогнозування*, процес *згладжування* часових рядів є певною мірою *суперечливою* процедурою.

- ✓ З одного боку наслідком згладжування є *зменшення ролі* випадкових чинників, що *не мають істотного* значення при формуванні змінної прогнозування.

Це, очевидно, є позитивним фактором та підвищує *якість отриманих прогнозів*.

- ✓ З іншого боку, *надмірне згладжування* може призвести до *втрати корисної інформації* про *фактичну тенденцію розвитку* прогнозованої змінної Y .

Не можна виключати, що «згладжені зміни» могли бути спричинені істотними для формування Y чинниками. Тобто «надмірне згладжування» може також *погіршувати* отримані прогнози.

В свою чергу, якість згладжування вихідного часового ряду значною мірою залежить від *правильного вибору* сталої згладжування k . Очевидно, що *меншим* значенням k відповідає «менший ефект» згладжування, *більшим* – *вищий*. Тому головну роль у «*правильному*» виборі сталої згладжування k при застосуванні методу «*повзучого тренду*» відіграють знання та досвід дослідника.

Часто, подібно до того, як це було у випадку вже розглянутих методів, вибір сталої згладжування k здійснюється *експериментальним шляхом*, тобто методом *послідовних емпіричних наближень*. Ця процедура буде проілюстрована далі, на конкретному прикладі.

3. Гармонічні ваги.

Визначення: Гармонічними вагами називаємо послідовність чисел:

$$H_1^n, H_2^n, \dots, H_n^n, n = 1, 2, \dots,$$

обчислених за формулами:

$$H_1^1 = 1;$$

$$H_1^n = 0, n > 1;$$

$$H_{t+1}^n = \frac{1}{n-1} \left[\frac{1}{n-1} + \frac{1}{n-2} + \dots + \frac{1}{n-t} \right],$$

$$n > 1, t = 1, 2, \dots, n-1.$$

Гармонічні ваги мають наступні властивості:

- Гармонічні ваги – це числа з інтервалу $(0, 1)$:

$$0 < H_t^n < 1, \text{ якщо } n > 1, \text{ та } t = 2, \dots, n.$$

- Для будь-якого $n > 1$ гармонічні ваги монотонно зростають:

$$0 = H_1^n < H_2^n < H_3^n < \dots < H_n^n.$$

- Для будь-якого $n > 1$ сума гармонічних ваг дорівнює одиниці

$$H_1^n + H_2^n + H_3^n + \dots + H_n^n = 1, n > 1.$$

Зауваження: При обчисленні гармонічних ваг корисним може бути наступне рекурентне співвідношення, що впливає безпосередньо з їх визначення:

$$H_{t+1}^n = H_t^n + \frac{1}{(n-1)(n-t)}, n > 1, t = 1, 2, \dots, n-1.$$

4. Точковий прогноз, що спирається на «гармонічні ваги».

Згладжений часовий ряд $\{y^*_1, y^*_2, \dots, y^*_n\}$, отриманий в результаті використання методу згладжування за допомогою *повзучого тренду*, може бути основою для прогнозування майбутніх значень досліджуваної змінної.

При визначенні прогнозу $y_{n+1,p}$ на майбутній період часу $(n + 1)$ використовується вся наявна інформація про досліджуване явище, що міститься в згладженому часовому ряді $\{y^*_1, y^*_2, \dots, y^*_n\}$, тому що всі ці значення беруть участь у обчисленні $y_{n+1,p}$.

Позначимо символом w_t визначений на підставі часового ряду приріст досліджуваної змінної Y в момент часу t :

$$w_t = y_t - y_{t-1}, t = 2, 3, \dots, n.$$

Тоді для будь-якого моменту часу t значення змінної прогнозування y_t можна визначити, додавши приріст w_t до її значення y_{t-1} в попередній момент $(t - 1)$:

$$y_t = y_{t-1} + w_t, t = 2, 3, \dots, n.$$

- Ідея методу «*гармонічних ваг*» полягає в оцінці на основі згладженого часового ряду $\{y^*_1, y^*_2, \dots, y^*_n\}$ *можливого приросту* w_{n+1} змінної прогнозування в момент $(n + 1)$.

Якщо символ $w_{n+1,p}$ позначає *прогноз* цього приросту, то значення прогнозу $y_{n+1,p}$ визначається додаванням прогнозного значення приросту $w_{n+1,p}$ до останнього значення y^*_n згладженого часового ряду.

Іншими словами:

$$y_{n+1,p} = y^*_n + w_{n+1,p}.$$

Практична реалізація цієї ідеї виглядає наступним чином.

- Спочатку, застосовуючи *метод повзучого тренду* до отриманого в результаті спостережень часового ряду $\{y_1, y_2, \dots, y_n\}$, одержуємо *згладжений часовий ряд*:

$$\{y^*_1, y^*_2, \dots, y^*_n\}.$$

- Після цього для послідовних періодів часу $t = 2, 3, \dots, n$, обчислюються прирости w^*_t за формулою:

$$w^*_t = y^*_t - y^*_{t-1}, t = 2, 3, \dots, n.$$

- На наступному кроці для забезпечення виконання постулату *старіння інформації* при визначенні прогнозованого значення приросту $w_{n+1,p}$ визначаємо послідовні значення *гармонічних ваг*.
- Тепер, використовуючи визначені послідовні значення гармонічних ваг, можемо обчислити прогноз $w_{n+1,p}$ приросту значення змінної Y на майбутній період часу $t = n + 1$.

З цією метою використовуємо знайдені раніше на підставі значень:

$$\{y^*_1, y^*_2, \dots, y^*_n\},$$

згладженого за допомогою *повзучого тренду* часового ряду, прирости: $\{w^*_2, w^*_3, \dots, w^*_n\}$.

- Прогноз $w_{n+1,p}$ обчислюємо, як середнє цих приростів, *зважає* гармонічними вагами:

$$w_{n+1,p} = w^*_2 \cdot H_2^n + w^*_3 \cdot H_3^n + \dots + w^*_n \cdot H_n^n, n > 1.$$

При цьому забезпечується виконання *постулату старіння інформації*, оскільки «новіші» прирости отримують *більші* ваги.

- Остаточно прогноз $y_{n+1,p}$ значення змінної Y в момент часу $t = n + 1$, що належить до майбутнього, визначаємо за формулою:

$$y_{n+1,p} = y^*_n + w_{n+1,p}.$$

5. Прогноз на базі «експоненціального згладжування».

Таким чином метод «повзучого тренду» передбачає *дві* чітко виражені фази *процесу прогнозування*:

- Фазу *діагностування минулого*, яка у випадку адаптивних моделей приймає форму «згладжування емпіричних даних»; та
- Фазу *визначення майбутнього*, тобто обчислення прогнозного значення для досліджуваної змінної.

Вони *розділені* одна від одної та реалізуються на практиці відповідно до *власних, окремих* алгоритмів.

Це створює можливість значно розширити множину різноманітних їх *модифікацій*.

Одним із напрямків такої модифікації є забезпечення *відповідної* до реальній ситуації *динаміки «старіння інформації»* в процесі прогнозування. В методі «повзучого тренду» це відбувається шляхом визначення прогнозованого значення приросту $w_{n+1,p}$:

- Прогноз $w_{n+1,p}$ обчислюємо, як *середнє-зважає* «гармонічними вагами» приростів $\{w^*_2, w^*_3, \dots, w^*_n\}$ згладженого за допомогою *повзучого тренду* часового ряду.

Прогноз $w_{n+1,p}$ приросту w_{n+1} в момент $n + 1$ можна визначити, наприклад, використовуючи «ваги методу експоненціального згладжування», що розглядався в [підрозділі 4.8](#).

Для заданих значень n та α послідовні значення:

$$h_2^n, h_3^n, \dots, h_{n-1}^n, h_n^n.$$

ваг методу *експоненціального згладжування* обчислюються за наступними формулами:

$$\begin{aligned}
 h_2^n &= (1 - \alpha)^{n-2}; h_3^n = \alpha(1 - \alpha)^{n-3}; \dots \\
 \dots; h_t^n &= \alpha(1 - \alpha)^{n-t}; \dots \\
 \dots; h_{n-1}^n &= \alpha(1 - \alpha); h_n^n = \alpha.
 \end{aligned}$$

Неважко перевірити, що для будь-якого числа $0 < \alpha < 1$, і для будь-якого n виконується рівність:

$$\begin{aligned}
 h_2^n + h_3^n + \dots + h_{n-1}^n + h_n^n &= \\
 = \alpha + \alpha(1 - \alpha) + \alpha(1 - \alpha)^2 + \alpha(1 - \alpha)^3 + \dots + \alpha(1 - \alpha)^{n-3} + (1 - \alpha)^{n-2} &= 1.
 \end{aligned}$$

Визначення. Величину $w_{n+1,p}$, яка обчислюється за формулою:

$$w_{n+1,p} = w_{n+1,p}^* \cdot h_2^n + w_{n+1,p}^* \cdot h_3^n + \dots + w_{n+1,p}^* \cdot h_{n-1}^n + w_{n+1,p}^* \cdot h_n^n.$$

будемо називати *середнім* приростів

$$\{w_{n+1,p}^*, w_{n+1,p}^*, \dots, w_{n+1,p}^*\}$$

згладженого часового ряду $\{y_{n+1,p}^*, y_{n+1,p}^*, \dots, y_{n+1,p}^*\}$, що «зважені» за допомогою експоненціальних ваг:

$$h_2^n, h_3^n, \dots, h_{n-1}^n, h_n^n.$$

- $w_{n+1,p}$ визначає прогноз *можливого приросту* w_{n+1} в момент $n + 1$. При цьому забезпечується виконання постулату старіння інформації, оскільки «новіші» прирости ($w_{n+1,p}^*$) отримують більші ваги.
- Остаточно прогноз $y_{n+1,p}$ значення змінної Y в момент часу $t = n + 1$, що належить до майбутнього, визначаємо за формулою:

$$y_{n+1,p} = y_{n+1,p}^* + w_{n+1,p}.$$

де $y_{n+1,p}^*$ – останнє значення згладженого часового ряду.

4.10. Точковий прогноз на основі «гармонічних ваг».

Приклад.

Наступний часовий ряд відображає попит на певний товар (*тис. шт.*) протягом року.

$$\begin{aligned}
 y_1 &= 26; y_2 = 25; y_3 = 31; y_4 = 23; y_5 = 32; y_6 = 31; \\
 y_7 &= 33; y_8 = 28; y_9 = 31; y_{10} = 33; y_{11} = 25; y_{12} = 27.
 \end{aligned}$$

На підставі цього ряду необхідно виконати *оперативне прогнозування* можливих чергових значень цього часового ряду, а саме:

- Обчислити *короткостроковий точковий прогноз*: $\{y_{13}^*, y_{14}^*, y_{15}^*\}$ попиту на цей товар на наступний квартал.

Для обчислення короткострокового прогнозу попиту в наступному кварталі скористатися методом «*товзучого тренду з постійним сегментом згладжування*» з використанням «гармонічних ваг».

Розв'язок: Вибір сталої згладжування k .

Використати з цією метою експериментальний метод, а саме:

- ✓ Доступні спостереження y_1, y_2, \dots, y_T ряду поділити на дві частини:

$$\{y_1, y_2, \dots, y_n\}; \{y_{n+1}, y_{n+2}, \dots, y_{n+m}\}; T = n + m;$$

$$\{1, 2, \dots, T\} = \{1, 2, \dots, n\} \cup \{n + 1, n + 2, \dots, n + m\}, T = n + m.$$

Отримані підмножини використати наступним чином:

- $\{1, 2, \dots, n\}$ – інтервал *побудови* прогностичної моделі;
 - $\{n + 1, n + 2, \dots, n + m\}$ – інтервал *емпіричної перевірки* прогнозу.
- ✓ Визначити наступний набір $K = [3; 4]$ можливих значень для ролі сталої згладжування.
- ✓ Для значень $k = 3$; та $k = 4$; провести наступні обчислення.

Побудова прогностичної моделі ($k = 3$).

Крок перший: «Згладжування» часового ряду y_1, y_2, \dots, y_n .

Вказівка: Припускаємо, що для *під-періодів*, які містять k спостережень, змінна прогнозування Y має *лінійний* характер. Тому на *першому кроці* вирівнювання часового ряду, щоб усунути випадкові коливання, параметри лінійних функцій тренду оцінюються для всіх послідовних фрагментів ряду з фіксованою довжиною k .

Завдання 1.

- 1) Поділити часовий ряд на послідовні відрізки довжини k :

$$(y_1, y_2, \dots, y_k); (y_2, y_3, \dots, y_{k+1}); \dots; (y_{n-k+1}, y_{n-k+2}, \dots, y_n).$$

- 2) Використовуючи функцію «ЛІНІЙНА» аркушу «Excel» побудувати відповідні функції лінійних трендів $f_i(t)$ для *непарних* значень $i = 1, 3, 5, \dots$:

$$f_1(t) = b_1 + a_1 \cdot t, t = 1, 2, \dots, k;$$

$$f_3(t) = b_3 + a_3 \cdot t, t = 3, 4, \dots, k + 1; \dots,$$

Відповідь. $(b_1, a_1) = (2,5, 22,3)$; $(b_3, a_3) = (0,5, 26,7)$;
 $(b_5, a_5) = (0,5, 29)$; $(b_7, a_7) = (-1, 38,7)$.

- 3) Використовуючи побудовані функції трендів $f_i(t)$ для *непарних* значень $i = 1, 3, 5, \dots$, обчислити відповідні теоретичні значення:

$$(\hat{y}_1^{(1)} = f_1(1), \hat{y}_2^{(1)} = f_1(2), \dots, \hat{y}_k^{(1)} = f_1(k));$$

$$(\hat{y}_3^{(3)} = f_3(3), \hat{y}_4^{(3)} = f_3(4), \dots, \hat{y}_{k+1}^{(3)} = f_3(k + 1)); \dots;$$

- 4) Використовуючи функцію «ТЕНДЕНЦІЯ» аркушу «Excel» обчислити відповідні теоретичні значення функції трендів $f_i(t)$ для *парних* значень i ,

$$(\hat{y}_2^{(2)} = f_2(2), \hat{y}_3^{(2)} = f_2(3), \dots, \hat{y}_{k+1}^{(2)} = f_2(k + 1)); \dots;$$

$$(\hat{y}_4^{(4)} = f_4(4), \hat{y}_5^{(4)} = f_4(5), \dots, \hat{y}_{k+3}^{(4)} = f_4(k + 3)); \dots,$$

5) Використовуючи функцію «СЕРЕДНС» аркушу «Excel» обчислити для кожного елемента (y_t) часового ряду відповідні їм згладжені значення (y_t^*).

Вказівка: Застосований принцип *повзучого тренду* створює ситуацію, коли деякі значення y_t часового ряду можуть бути спільними одночасно для кількох сегментів згладжування. Для визначення згладжених значень використати наступну формулу:

$$y_t^* = \frac{1}{1 + g(t) - d(t)} \sum_{j=d(t)}^{g(t)} f_j(t), \quad t = 1, 2, \dots, n,$$

$$d(t) = \begin{cases} 1, & \text{для } t = 1, 2, \dots, k \\ t - k + 1, & \text{для } t = k + 1, \dots, n \end{cases};$$

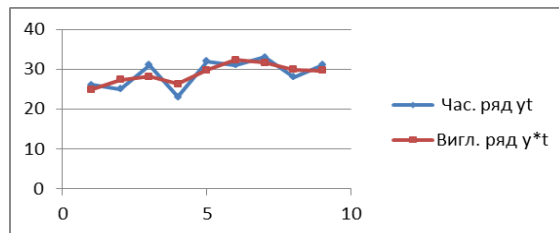
$$g(t) = \begin{cases} t, & \text{для } t = 1, 2, \dots, n - k + 1 \\ n - k + 1, & \text{для } t = n - k + 2, \dots, n \end{cases}.$$

Відповідь: $y_1^* = 24,83$; $y_2^* = 27,33$; $y_3^* = 28,11$; $y_4^* = 26,22$;
 $y_5^* = 29,78$; $y_6^* = 32,28$; $y_7^* = 31,61$; $y_8^* = 29,92$; $y_9^* = 29,67$.

Завдання 2. Побудувати графік «згладженої» за допомогою *повзучого тренду* тенденції розвитку часового ряду y_1, y_2, \dots, y_n . З цієї метою:

Побудувати в аркуші «Excel» відповідну точкову діаграму, що послідовно з'єднує точки $\{(1, y_1^*), (2, y_2^*), \dots, (n, y_n^*)\}$ прямими відрізками.

Отримана ломана лінія буде представляти «згладжену» за допомогою *повзучого тренду* тенденцію розвитку часового ряду y_1, y_2, \dots, y_n .



Крок другий: Прогнозування в інтервалі емпіричної перевірки.

Вказівка: Ідея методу *гармонічних ваг* полягає в побудові прогнозу можливого приросту:

$$w_{n+1} = y_{n+1} - y_n$$

змінної Y в момент $n + 1$.

Якщо символ $w_{n+1,p}$ позначає *прогноз* цього приросту, то значення прогнозу $y_{n+1,p}$ визначається за формулою:

$$y_{n+1,p} = y_n^* + w_{n+1,p}.$$

де y_n^* – останнє значення згладженого часового ряду.

Завдання 3. Обчислити для послідовних періодів часу $t = 2, 3, \dots, n$, прирости $\{w_t^*, t = 2, 3, \dots, n\}$ «згладженого» за допомогою повзучого тренду часового ряду y_1, y_2, \dots, y_n за формулою:

$$w_t^* = y_t^* - y_{t-1}^*, t = 2, 3, \dots, n.$$

Відповідь: $w_2^* = 2,5$; $w_3^* = 0,78$; $w_4^* = -1,89$; $w_5^* = 3,56$;
 $w_6^* = 2,5$; $w_7^* = -0,67$; $w_8^* = -1,69$; $w_9^* = -0,25$.

Крок третій: Обчислення значень гармонічних ваг.

Завдання 4. Визначити послідовні значення гармонічних ваг:

$$H_1^n, H_2^n, \dots, H_n^n, n = 1, 2, \dots$$

Для цього скористатися наступним алгоритмом:

$$\checkmark n = 1: H_1^1 = 1;$$

$$\checkmark n > 1:$$

$$H_1^n = 0;$$

$$H_{t+1}^n = \frac{1}{n-1} \left[\frac{1}{n-1} + \frac{1}{n-2} + \dots + \frac{1}{n-t} \right], t = 1, 2, \dots, n-1.$$

Відповідь: $H_1^9 = 0$; $H_2^9 = 0,016$; $H_3^9 = 0,033$; $H_4^9 = 0,054$;
 $H_5^9 = 0,079$; $H_6^9 = 0,111$; $H_7^9 = 0,152$; $H_8^9 = 0,215$; $H_9^9 = 0,34$.

Вказівка: При обчисленні гармонічних ваг можна використати наступне рекурентне співвідношення:

$$H_{t+1}^n = H_t^n + \frac{1}{(n-1) \cdot (n-t)}, n > 1, t = 1, 2, \dots, n-1.$$

Завдання 5. Перевірити для отриманих значень гармонічних ваг виконання наступного співвідношення:

$$H_{t+1}^n - H_t^n = \frac{1}{(n-1)(n-t)}, n > 1, t = 1, 2, \dots, n-1.$$

Емпірична перевірка точності прогнозів ex-post.

Крок четвертий: Обчислення прогнозу ex-post $y_{n+1,p}$.

Завдання 6. Використовуючи гармонічні ваги та обчислені в завданні 3 прирости $\{w_t^*, t = 2, 3, \dots, n\}$ «згладженого» часового ряду визначити прогноз $w_{n+1,p}$ можливого приросту w_{n+1} в момент $n+1$ за формулою:

$$w_{n+1,p} = w_2^* \cdot H_2^n + w_3^* \cdot H_3^n + \dots + w_n^* \cdot H_n^n, n > 1.$$

Завдання 7. Визначити прогноз $y_{n+1,p}$, змінної прогнозування Y на момент часу $n+1$ за формулою:

$$y_{n+1,p} = y_n^* + w_{n+1,p},$$

де y_n^* – останнє значення згладженого часового ряду.

Відповідь: $y_{10,p} = 29,637$.

Завдання 8. Визначити прогнози $\{y_{n+i,p}, i = 2, 3, \dots, m\}$, змінної прогнозування Y на моменти часу $\{n+2, n+3, \dots, n+m\}$, що належать до інтервалу *емпіричної перевірки* прогнозу; за формулою:

$$y_{n+i,p} = y_{n+i-1,p} + w_{n+i,p},$$

де $y_{n+i-1,p}$ – попередній прогноз з цього інтервалу.

Відповідь: $y_{11,p} = 29,608$; $y_{12,p} = 29,579$.

Крок п'ятий: Оцінка точності прогнозів *ex-post* $\{y_{n+i,p}, i = 1, 2, \dots, m\}$.

Завдання 9. Використовуючи ту частину доступних спостережень:

$$\{y_{n+1}, y_{n+2}, \dots, y_{n+m}\}$$

часового ряду, які належать до інтервалу *емпіричної перевірки* прогнозу, та обчислені прогнози:

$$\{y_{n+1,p}, y_{n+2,p}, \dots, y_{n+m,p}\},$$

обчислити наступні показники помилки прогнозу *ex post* в інтервал *емпіричної верифікації*:

1. *Середню безумовну абсолютну похибку* прогнозу *ex-post*:

$$MAE = \frac{1}{m} \cdot \sum_{t=1}^m |y_{n+t} - y_{n+t,p}|.$$

2. *Середньо-квадратичну* помилку прогнозу *ex-post* :

$$S^2 = MSE = \frac{1}{m} \cdot \sum_{t=1}^m (y_{n+t} - y_{n+t,p})^2.$$

3. $U^M = \frac{(\bar{y} - \bar{y}_p)^2}{MSE}$, де $\bar{y} = \frac{1}{m} \cdot \sum_{t=1}^m y_{n+t}$ та $\bar{y}_p = \frac{1}{m} \cdot \sum_{t=1}^m y_{n+t,p}$.

4. $U^S = \frac{(\sigma_y - \sigma_{y_p})^2}{MSE}$; де $\sigma_y = \sqrt{\sigma_y^2}$ та $\sigma_{y_p} = \sqrt{\sigma_{y_p}^2}$, а

$$\sigma_y^2 = \frac{1}{m} \cdot \sum_{t=1}^m (y_{n+t} - \bar{y})^2; \text{ та } \sigma_{y_p}^2 = \frac{1}{m} \cdot \sum_{t=1}^m (y_{n+t} - \bar{y}_p)^2$$

Відповідь: $MAE_{(k=3)} = 3,516$; $MSE_{(k=3)} = 13,064$; $U^M_{(k=3)} = 0,002$; $U^S_{(k=3)} = 0,872$.

Зауваження: Обчислення, проведені для значення сталої згладжування $k = 4$ дали наступні результати:

Відповідь: $MAE_{(k=4)} = 3,783$; $MSE_{(k=4)} = 15,3$; $U^M_{(k=4)} = 0,222$; $U^S_{(k=4)} = 0,724$.

Крок шостий: Вибір сталої згладжування k .

Завдання 10. В якості остаточного критерію для вибору сталої згладжування $k \in K$, серед можливих її значень з множини $k \in K = [3; 4]$, застосувати синтетичний показник: $\Sigma = MAE + S + U^M$, де $S = \sqrt{S^2} = \sqrt{MSE}$.

- «Найбільш точним» будемо вважати прогноз *ex post* для того значення $k \in K = [3; 4]$, для якого Σ є мінімальною.

$$\Sigma_3 = MAE_3 + S_3 + U_3^M = 3,516 + 3,614 + 0,124 = 7,255;$$

$$\Sigma_4 = MAE_4 + S_4 + U_4^M = 3,783 + 3,912 + 0,222 = 7,916;$$

$$\min(\Sigma_3; \Sigma_4) = \min(7,255; 7,916) = 7,255 = \Sigma_3 \Rightarrow k = 3.$$

Висновок: Значення $k = 3$ вибирається, як стала згладжування методу «повзучого тренду з постійним сегментом згладжування» з використанням «гармонічних ваг» для побудови «прогнозів *ex-ante*» невідомих значень прогнозованої змінної Y .

Період прогнозування у цьому випадку належить до майбутнього, а отже є недоступним для спостереження.

Відповідь: Стала згладжування методу «повзучого тренду» для даного прикладу дорівнює $k = 3$.

4.11. Технічний аналіз в економічних дослідженнях.

1. Головний принцип побудови методів технічного аналізу. 2. Постулати теорії технічного аналізу К. Доу. 3. Тренд та тенденція. 4. Тенденція розвитку явищ в технічному аналізі. 5. Головні принципи прийняття рішень в технічному аналізі.

1. Головний принцип побудови методів технічного аналізу.

В 70-х роках минулого століття на основі окремих фрагментів, тобто методів технічного аналізу призначених для вирішення конкретних практичних завдань, була створена цілісна і універсальна теорія, об'єднана єдиною ідеологією, філософією, аксіомами та загальними принципами.

- Основний серед цих принципів, який стосується економічних процесів, передбачає, що динаміка цих процесів підпорядковується строгим закономірностям, які з великою ймовірністю проявляться в майбутньому.

На будь-яке економічне явище може впливати дуже велика кількість різноманітних факторів. Технічний аналіз дозволяє уникнути *детального* вивчення окремих складових та їх взаємозв'язків. Методи технічного аналізу розглядають це явище у *повному* обсязі (в цілому) як кінцевий результат взаємодії окремих чинників, що його формують.

Неважко помітити, що цей принцип дуже подібний до того, який використовується при побудові моделей часових рядів, з однією, однак, суттєвою відмінністю:

- При побудові методів, призначених для аналізу *часових рядів*, використовуються *математичні засоби*, що класифікуються як *аналітичні*.
- Основними інструментами *технічного аналізу* є різні типи *діаграм і таблиць* (звідси назва «технічний аналіз»).

Стисло технічний аналіз можна визначити наступним чином:

- Це метод підготовки економічних прогнозів (включно з прогнозами кон'юнктури) шляхом *побудови* та належної *інтерпретації* відповідних графіків для періодів часу, що належать минулому.

При цьому *побудову* та *інтерпретацію* діаграм на основі емпіричних даних про конкретні явища слід розглядати як *специфічний аналіз цих явищ*.

- Отримані графіки відображають внутрішні *технічні* параметри, притаманні явищам, що вивчаються, дозволяють побачити *результат взаємодії* різноманітних факторів, що на них впливають, а отже *встановити закономірності* їх розвитку.

Тому технічний аналіз – це не тільки дійові методи *прогнозування* економічних процесів, але й ефективний інструмент *економічного аналізу*.

2. Постулати теорії технічного аналізу К. Доу.

Початком історії розвитку «*Теорії технічного аналізу*», що нині розглядається як самостійна галузь наукових досліджень, та окрема, *спеціальна методологія*, яка використовується в економічних науках, вважається публікація у 1890 р. статті К. Доу, в якій були введені основні *поняття* та сформульовані основні *постулати* технічного аналізу.

Пізніше ідеї, сформульовані в згаданій статті, знайшли суттєвий розвиток у роботах Р. Н. Еліота, який створив *математично-досконалу*, послідовну та універсальну теорію *циклічного розвитку природних явищ*.

- Варто зауважити, що принципи *циклічності розвитку* мають універсальний характер та стосуються явищ будь-якої природи.

Ця теорія може бути використана при вивченні економічних явищ, зокрема ринкової *кон'юнктури*.

Розглянемо їх на прикладі процесу динаміки цін на фондовому ринку. Такий вибір зроблено з двох причин:

- Перш за все головним предметом дослідження в цьому навчальному курсі є *криптовалюта*.

Ринок криптовалют – це *окремий сегмент* фінансового ринку, а будь-яка крипто валюта – *інструмент* на фондовому ринку.

- Технічний аналіз – один з ефективних інструментів дослідження крипторинку, що широко використовується на практиці.
- З іншого боку, можливість інтерпретації всіх теоретичних понять на *конкретних прикладах* суттєво полегшить розуміння головних принципів теорії та дозволить *уникнути абстрактних* міркувань.

Сформулюємо основні припущення технічного аналізу:

1. Перше припущення:

- Графік, який показує динаміку досліджуваного явища, враховує всі фактори, що формують це явище.

2. Друге припущення:

- Динаміка розвитку природних явищ (включаючи також явища економічні) – це спрямований рух.

3. Третє припущення:

- Розвиток природних явищ – це циклічний процес, при цьому хвиля динаміки повторюється.

3. Тренд та тенденція.

Поняття *тренду* та *тенденції* відіграють ключову роль у цій теорії. У попередніх лекціях ці терміни вже використовувалися багато разів, але зараз ми маємо можливість їх конкретизувати.

- Тренд характеризує *поточний напрямок* зміни досліджуваного явища.

Зазвичай існує три типи трендів:

- Рух *вгору*, або в біржовій термінології – *бичачий тренд*;
- Відсутня помітна зміна, тобто *бічний рух*, що вказує на збереження майже постійного рівня;
- Рух *вниз*, або в термінології фондової біржі – *ведмежий тренд*.

Згідно з теорією Доу, існує також три відповідні типи тенденції: «*бичача*»; «*бічна*» та «*ведмежа*».

Варто підкреслити, однак, що насправді жодна з розглянутих вище тенденцій не спостерігається у «*чистому*» вигляді, тобто у формі «*руху по прямій*» у конкретному напрямку.

Тому згідно з теорією К. Доу, *тенденцію* визначають наступним чином:

- Враховуючи циклічний характер розвитку, тенденція буде залишатися зростаючою до тих пір, поки кожен наступний «*пік*» і кожне наступне «*дно*» графіка хвилі буде *вище* попереднього.

Іншими словами, висхідна тенденція (тобто в біржовій термінології - *бичача*) повинна мати форму кривої з *послідовно зростаючими* локальними *екстремальними* значеннями: як *максимальними*, так і *мінімальними*.

- У випадку тенденції *спадкової* (до *зниження*), тобто *ведмежої* в біржовій термінології, кожен наступний «*пік*» і кожне наступне «*дно*» графіка хвилі буде *нижчим* за попередній.

Одне з основних припущень теорії та методології технічного аналізу, що стосується взаємозв'язку між поняттями «*тренд*» та «*тенденція*», можна сформулювати таким чином:

- *Тренд* рухається в тому ж самому напрямку до тих пір, поки *тенденція* не змінить свій напрямок на протилежний.

4. Тенденція розвитку явищ в технічному аналізі.

Припущення про взаємозв'язок між поняттями «тренд» та «тенденція» є вихідним пунктом для вивчення *тенденцій розвитку* явищ з використанням методів технічного аналізу.

Описуючи один завершений цикл, що охоплює одну повну хвилю, теорія Доу розрізняє три категорії тенденцій:

1. *Первинна* тенденція. 2. *Вторинна* тенденція. 3. *Мала* тенденція.

Дамо коротку характеристику кожної з них, ілюструючи (при можливості) на прикладі фондового ринку.

1. Первинна тенденція, або інакше – *основна* тенденція, є визначальною тенденцією в даній хвилі, в тому сенсі, що вона триває *найдовше* за весь цикл цієї хвилі.

Первинна тенденція, у свою чергу, має три фази:

➤ *Перша* фаза, тобто фаза *накопичення* (ang. *accumulation*).

Що стосується, наприклад, фондового ринку, то ця фаза визначає період, коли найбільш *передбачливі* інвестори вирішують, що всі негативні, несприятливі новини вже були поглинені та прийняті фондовим ринком і *починають купувати* цінні папери.

➤ *Друга* фаза, тобто фаза *пожвавлення*.

На фондовому ринку ця фаза починається тоді, коли, намагаючись не відставати від основної тенденції, більшість «*гравців*» починають купувати цінні папери. Це особливо стосується тих, хто використовує *методи технічного аналізу*.

- Характерною особливістю цієї фази є те, що *ціни швидко ростуть*, а атмосфера стає все більш *оптимістичною*.

➤ *Третя* фаза, тобто фаза *ажіотажу*.

На фондовому ринку фаза *пожвавлення* плавно переходить у фазу *ажіотажу*. Купувати цінні папери починають широкі верстви громадян.

- Ця фаза характеризується тим, що «*поінформовані*» інвестори, тобто найбільш здатні до передбачення майбутнього, які першими відчули момент *зміни* на ринку *ведмежої* тенденції і почали купувати цінні папери, починають їх *продавати*.

Це робиться тоді, коли більшість, навпаки, хоче їх придбати.

2. Вторинна тенденція (відома також як *проміжна*) – коригує основну тенденцію.

- Тривалість цієї корекції коротша, ніж основна тенденція. Загалом вона може становити від 1/3 до 2/3 тривалості попередньої тенденції.

3. Мала (*короткочасна*) тенденція – це короткострокові коливання, що виникають у межах вторинної тенденції, тобто під час корекції основної тенденції.

5. Головні принципи прийняття рішень в технічному аналізі.

Основний принцип технічного аналізу можна сформулювати наступним чином:

- Якщо маємо декілька різних *аналогічних* показників, то для того, щоб можна було приймати рішення на їх основі, *показники повинні бути узгоджені* один з одним.

Проілюструємо цей принцип на прикладі фондового ринку.

- Основна мета прогнозування біржових процесів – це завдання *відгадати* момент «перелому», тобто момент зміни напрямку існуючої тенденції.

Важливим показником напрямку основної тенденції, що завжди рухається згідно з нею, є *рівень товарообігу*.

- Отже зміна основного напрямку тенденції також повинна підтверджуватися рівнем продажів.

Наступний фундаментальний постулат технічного аналізу, який в певному сенсі є продовженням попереднього, відображає *масовий характер причин*, що формують основну тенденцію. Його можна сформулювати наступним чином:

- Тенденція, яка розпочала свій рух, буде прагнути його продовження.

Іншими словами:

- Зміна напрямку існуючої тенденції повинна бути підтверджена *значними, достовірними* сигналами.

Через дуже велику кількість суб'єктів господарювання, що діють на ринках, та ще більшу кількість можливих факторів, які можуть впливати на ці суб'єкти господарювання, *точний фундаментальний аналіз* цих ринків практично *неможливий*.

В той же час, технічний аналіз, який враховує сукупний вплив усіх факторів одночасно, може бути дуже *точним, ефективним* та *дієвим*.

Мистецтво прогнозування *кон'юнктури* (у випадку, коли ми говоримо про біржові процеси), полягає на тому, щоб:

- *Вгадати* момент «перелому».

Або іншими словами:

- Здатність *відрізнити* звичайну проміжну *корекцію* основної тенденції від *зміни* її напрямку на зворотній.

З цієї точки зору прості та дешеві засоби технічного аналізу можуть бути дуже ефективними. Безперечно, однак, що найкращого ефекту можна досягти, якщо *системно* поєднувати *технічні* засоби з методами фундаментального аналізу, що певним чином *доповнюють* один одного.

4.12. «Хвильова діаграма Еліота» в технічному аналізі.

1. Теорія циклічного розвитку Р. Н. Еліота.
2. Хвильова діаграма.
3. Універсальний характер теорії Еліота.
4. Графічний інструментарій технічного аналізу.
5. Механічні методи в технічному аналізі

1. Теорія циклічного розвитку Р. Н. Еліота.

В попередньому підрозділі підкреслювалось, що започаткована К. Доу «Теорія технічного аналізу» знайшла свій подальший розвиток в працях Р. Н. Еліота. Йому вдалося трансформувати створене К. Доу «принципове ядро» новітньої теорії у змістовну, послідовну, строгу, високоефективну і, що дуже важливо, універсальну *математичну дисципліну*.

Еліот *строго-математично* обґрунтував хвильовий характер розвитку багатьох явищ, зокрема динаміки *короткострокової кон'юнктури*, сформулювавши тим самим основну концепцію технічного аналізу. «Теорія хвиль» технічного аналізу, створена Еліотом, існує майже без змін і сьогодні. Має вона багато прихильників і все ширше використовується в різних сферах, особливо в економіці.

Варто підкреслити своєрідну *довершеність*, чи *досконалість*, створеної Еліотом теорії. Ця *довершеність* полягає в тому, що подальший розвиток теорії не стосується *корекції*, або *вдосконалення* її основних положень.

➤ Він полягає в їх *деталізації* та відбувається шляхом *чіткого* їх тлумачення і *правильної* інтерпретації в різних *конкретних практичних* ситуаціях.

Завдяки економічним застосуванням теорію Еліота можна розглядати як одну із перших успішних спроб використання *строгих* кількісних *математичних* методів для аналізу масових соціально-економічних явищ в умовах *невизначеності*, які дуже важко описати формальним чином.

Згідно з концепцією Еліота, динаміка розвитку таких процесів нагадує поведінку «*натовпу*», тобто проходить кілька специфічних фаз, які можна умовно визначити наступним чином:

- Фаза «*експансії*»;
- Фаза «*ентузіазму*»;
- Фаза «*ейфорії*»;
- Фаза «*заспокоєння*»;
- Фаза «*занепаду*»;
- Фаза «*депресії*».

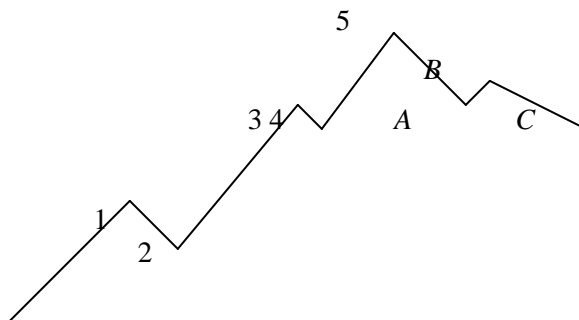
Для різних явищ подібні хвилі відрізняються лише тривалістю всієї хвилі та окремих фаз і їх амплітудою.

2. Хвильова діаграма.

Основним елементом хвильової теорії Еліота є графік, який називається *хвильовою діаграмою*. Ця діаграма в певному сенсі уточнює та конкрети-

зує основні теоретичні положення К. Доу. Хвильова діаграма Еліота має вигляд, представлений на малюнку 1.

Як і вся теорія Еліота, ця діаграма є *універсальною* і при правильній інтерпретації її можна використовувати в різних практичних ситуаціях для опису явищ різної природи. Але в даному випадку будемо інтерпретувати її з точки зору процесів, що відбуваються в *фінансовій сфері*, а точніше на *ринку цінних паперів*.



Малюнок 1. Хвильова діаграма Еліота.

Головна або основна тенденція в теорії Доу (див. [підрозділ 4.11](#)) представлена на цій діаграмі у вигляді п'яти хвиль, позначених цифрами (1, 2, 3, 4, 5).

- **Хвиля 1.** Це еквівалент *першої* фази (*фази накопичення*) в теорії Доу.

Ця хвиля відповідає періоду зміни ведмежої *тенденції* на бичачий, коли все ще переважають настрої невизначеності, страху і лише найбільш «далекоглядні», «поінформовані» та «відважні» гравці, які точно відчували момент «перелому» на фінансовому ринку, починають активно скуповувати цінні папери.

- **Хвиля 2.** Коротка і в той же час досить «глибока» хвиля (еквівалент невеликого «коректування» тренду).

Ця хвиля неминуче слідує за першою висхідною хвилею і характеризується тим, що деякі інвестори, побоюючись повернення ведмежої тенденції, починають продавати придбані цінні папери.

- **Хвиля 3.** Вирішальна, ключова хвиля *основної тенденції* з найбільшою тривалістю, еквівалент *другої* фази в теорії Доу.

Ця хвиля характеризується постійним зростанням вартості цінних паперів, що супроводжується підвищенням рівня продаж. Це найкращий час для розміщення контрактів на фінансових ринках. Саме ця *третья* хвиля із п'яти можливих, дозволяє чітко і однозначно визначити основну тенденцію.

- **Хвиля 4.** Коротка і зазвичай не дуже глибока низхідна хвиля, яка сигналізує про те, що фінансовий ринок вже «втомився» і в певному сенсі «ресурси» основної тенденції добігають кінця.
- **Хвиля 5.** Остання, третя фаза основної тенденції.

Ця хвиля може бути досить тривалою в часі, але зростання ціни вже не таке стрімке, як під час хвилі 3. При цьому кількість продажів та рівень товарообігу характеризуються помітним спаданням.

Це пов'язано з тим, що «професіонали», тобто найбільш «обізнані» гравці вже відчули момент «перелому» на фінансовому ринку і починають продавати цінні папери, придбані під час **хвилі 1**.

Висхідний характер цієї хвилі можна пояснити інерцією фінансового ринку, спричиненою діяльністю на цьому ринку «аматорів», залучених у «гру» під час 3-ї хвилі.

Хвилі *A*, *B*, *C*, відповідно до класифікації в теорії Доу, утворюють *вторинну*, тобто *коригувальну* тенденцію.

- **Хвиля А.** Ця хвиля неминуче йде за хвилею 5 і характеризується тим, що «досвідчена» частина інвесторів, яка правильно вгадала момент *обвалу* (тобто «перелому») на фінансовому ринку і закінчення бичачої тенденції, активно і масово продає свої цінні папери.

Інша, більш чисельна, але менш «досвідчена» частина гравців, сприймаючи падіння на фінансовому ринку, як тимчасову корекцію цін, продовжує скуповувати цінні папери.

- **Хвиля В.** Коротка спроба фінансового ринку відновитися, яка, однак, не закінчується успіхом.

Більшість інвесторів намагаються запобігти можливим збиткам і хоча б частково компенсувати понесені витрати, тобто починають масово *продавати* свої цінні папери, які швидко дешевшають.

- **Хвиля С.** Це повернення на фінансовий ринок *ведмежої тенденції*.

Хвилі *A* та *B* викликають на фінансовому ринку досить довгу хвилю *C*. За тривалістю та з точки зору процесів, що відбуваються на фінансовому ринку, хвилю *C* можна порівняти з хвилею 3: вона дозволяє чітко і однозначно визначити його основний характер, а саме – зміну *бичачої* тенденції на *ведмежий*.

3. Універсальний характер теорії Еліота.

Еліот вважав, що його хвильова теорія має *загальний* та *універсальний* характер. При цьому представлена вище «хвильова діаграма» відіграє в цій теорії роль «*елементарної частинки*».

На думку Еліота, циклічність масових процесів полягає в тому, що «*елементарні*» хвилі Еліота поєднуються і створюють подібні хвилі

більшого розміру, що описують циклічні процеси на більш високому рівні загальності.

В свою чергу, ці «хвилі більшого розміру» є «елементарними частинками» хвиль ще більшого розміру на наступному рівні, ітд.

Результатом такого «*поступового агрегування*» є правдивий опис поточних реальних процесів, у тому числі і *економічних*. Така інтерпретація циклічних процесів і побудова хвилі Еліота дозволяє краще зрозуміти співвідношення понять «*тренд*» і «*тенденція*»:

- Хвилі «*елементарних*» хвильових діаграм, що утворюють *агреговану* хвилю, яка описує досліджуване явище в його цілісності, представляють «*тренди*» в певних часових інтервалах.
- Тоді як на сукупній, *агрегатній* хвильовій діаграмі Еліота видно основну «*тенденцію*» розвитку явища, що досліджується.

На ній можна визначити *тип* актуальної тенденції, її *фазу* тощо.

Заслугою Еліота є також те, що, крім уточнення теоретичних положень, сформульованих Доу, він не тільки запропонував конкретну *форму* і *структуру* хвилі, що описує циклічні процеси природи, але й визначив чіткі *кількісні пропорції* між тривалістю окремих фаз цієї структури. Для ознайомлення з конкретними числовими аспектами технічної теорії Еліота відсилаємо зацікавлених читачів до спеціальної літератури з цього питання. Не вдаючись в деталі відзначимо лише, що в теорії Еліота основним математичним інструментом для визначення таких пропорцій є послідовність чисел Фібоначчі $\{f_1, f_2, \dots, f_n, \dots\}$.

У математичній теорії чисел така послідовність визначається рекурентним чином:

- Перші два члени послідовності Фібоначчі дорівнюють одиниці:

$$f_1 = 1; f_2 = 1.$$

- Кожен член f_n послідовності Фібоначчі дорівнює сумі двох його попередніх членів, тобто мають місце наступні рівності:

$$f_n = f_{n-2} + f_{n-1}, n = 3, 4, 5, \dots$$

Так, наприклад, перші кілька членів послідовності Фібоначчі дорівнюють:

$$\begin{aligned} f_1 &= 1, f_2 = 1, \\ f_3 &= f_1 + f_2 = 1 + 1 = 2, f_4 = f_2 + f_3 = 1 + 2 = 3, \\ f_5 &= f_3 + f_4 = 2 + 3 = 5, f_6 = f_4 + f_5 = 3 + 5 = 8, \\ f_7 &= f_5 + f_6 = 5 + 8 = 13, f_8 = f_6 + f_7 = 8 + 13 = 21, \\ f_9 &= f_7 + f_8 = 13 + 21 = 34, \dots, \text{ітд.} \end{aligned}$$

4. Графічний інструментарій технічного аналізу.

Основним інструментом технічного аналізу є спеціальні види графіків та діаграм. При цьому технічний аналіз значною мірою буде свої прогнози

на детальному опрацюванні та ретельному їх вивченні. Це дозволяє виділити окремі фрагменти цих діаграм та дати їм відповідну інтерпретацію.

В якості прикладу використання таких «фрагментів графіків» при вивченні ситуації на фондовому ринку можна привести різні види поєднання елементів діаграми в конкретні «фігури», або інакше – «формації». Так для визначення моменту зміни тенденції або підтвердження продовження існуючої тенденції, використовуються «формації», що дістали назву «голова та плечі», «прапор», «вимпел», «трикутник» тощо.

Крім найпростіших відомих у елементарній математиці лінійних графіків або «стовпчикових» діаграм, технічний аналіз використовує також більш складні, як наприклад, «фігурні діаграми», «японські свічки» тощо. Цьому служать також певні, побудовані спеціальним чином на графіках лінії (так звані «опорні лінії»).

5. Механічні методи в технічному аналізі.

Дуже корисними при визначенні економічних прогнозів кон'юнктури можуть бути «згладжені» із застосуванням «механічних» методів графіки динаміки досліджуваних циклічних процесів. Такі «згладжені лінії» можна побудувати використовуючи, наприклад, механічні методи «ковзного середнього», «експоненціального згладжування», тощо.

Зазвичай «згладжені» лінії будуються на тому ж графіку, що й реальні лінії динаміки, а взаємне розташування «згладжених» і реальних ліній може дати багато корисної інформації для прогнозування розвитку розглянутих явищ. У технічному аналізі, наприклад, діє таке правило:

- Якщо «згладжена» лінія розташована нижче лінії динаміки, то тенденція буде висхідною (тобто в біржовій термінології – бичачий тренд);
- Якщо ж ця лінія розташована вище лінії динаміки, то тенденція буде низхідною (тобто в біржовій термінології – ведмежий тренд).

При цьому:

- Точки перетину реальної лінії динаміки зі «згладженою» слід розглядати як «моменти заломлення», тобто моменти зміни напрямку тенденції.

Практика дослідження кон'юнктури та складання економічних прогнозів свідчить про високу ефективність правильного застосування подібних принципів. Тобто при побудові таких прогнозів необхідно враховувати своєрідне «відставання» або «запізнення» на «згладжених лініях» певних «характерних» для реальних процесів точок (особливо у випадку «бічних трендів»).

Інший тип «спеціальних» кривих, що полегшують визначення прогнозів кон'юнктури, це діаграми, які називаються *осциляторами*. Будуються вони також за допомогою «механічних» методів, а підставою для їх створення можуть бути, зокрема, різноманітні показники динаміки (*прирости, індекси*, тощо).

Наведемо приклади найпростіших, однак досить ефективних з практичної точки зору, осциляторів.

- Осцилятор *моментів* ($m_t^{(x)}$).

Цей осцилятор визначається на основі *абсолютних приростів*. Нехай y_t , $t = 1, 2, \dots$ означає динамічний (*часовий*) ряд, що описує досліджуване явище; x означає деяке заздалегідь визначене число. Тоді осцилятор моментів визначається наступним чином:

$$m_t^{(x)} = y_t - y_{t-x}, t = x + 1, x + 2, \dots$$

- Осцилятор ($i_{t/t-x}$), що дістав назву «*рівень змін*», визначається на основі *індексів динаміки*. $i_{t/t-x} = y_t / y_{t-x}$, $t = x + 1, x + 2, \dots$, тощо.

На відміну від «*згладжених*» (тобто «*усереднених*») ліній, які зазвичай будуються на тому ж графіку, що й «*реальні*» лінії динаміки, при використанні осциляторів, осциляторні діаграми будуються на іншому, спеціально підготовленому для цього графіку. На ньому, крім осцилятора, позначаються також «*лінії*» спеціальним чином визначених «*рівнів*».

- Моменти перетину осциляторами цих «*ліній*» вказують на появу певних «*подій*», прогнозування яких є метою дослідження.

Іншими словами, аналізуючи такі графіки отримуємо, зокрема, необхідну *інформацію* для прогнозування «*моментів заломлення*», тобто моментів *зміни напрямку* основної тенденції.

Наступна відмінність використання осциляторів стосується ефекту «*запізнення усереднених ліній*». На відміну від прогнозу «*моментів заломлення*» основної тенденції за допомогою «*згладженої лінії*», яка зазвичай трохи «*затримується*», прогноз, визначений на основі осциляторів, як правило, є «*випереджаючим*», тобто сигналізує про момент зміни напрямку тренда раніше, ніж це насправді має місце.

Вищезазначені коментарі, серед іншого, підтверджують сформульований в попередньому підрозділі «*основний принцип*» технічного аналізу та свідчать про те, що найбільш продуктивним та ефективним є системне використання методів технічного аналізу:

- Тобто *одночасне* застосування кількох різних *аналогічних* показників;
- *Порівняння* отриманих результатів;
- *Узгодженість* цих результатів, як підстава до прийняття рішення.

На закінчення варто відзначити, що практика використання теорії Еліота чітко і переконливо підтвердила її високу ефективність і високу результативність. Це, в першу чергу, стосується використання методів технічного аналізу для дослідження стану та визначення прогнозів кон'юнктури економічних ринків (зокрема *фінансових*).

Але це далеко не єдина сфера їх успішного використання – багато інших складних соціально-економічних явищ досліджується є допомогою методів технічного аналізу.

4.13. Модель тенденції розвитку: точність прогнозів.

Економетрико-статистичні методи в дослідженні економічних процесів.

1. Лінійна модель – статистичні припущення. 2. Помилка прогнозу (лінійна модель). 3. Інтервал певності для прогнозованих значень. 4. Оцінка точності (нормальний розподіл). 5. Прогнозований інтервал на підставі t -розподілу.

В підрозділах 3.10 – 3.13; 4,4 ілюструвалась можливість використання моделей тенденції розвитку (як лінійних, так і нелінійних) до аналізу економічних явищ. На прикладі аналізу динаміки національного доходу було показано, яким чином можна використати з цією метою економічні часові ряди:

- З їх допомогою можна, з одного боку, будувати адекватні аналітичні моделі, що описують подібні явища, а отже отримувати можливість її *ефективного аналізу*;
- З іншого боку, спираючись на ці моделі, створювати надійні інструменти передбачення та прогнозу їх можливого розвитку.

В підрозділі 3.12, спираючись на числові дані

$$V_1 = 416,5; V_2 = 444,2; V_3 = 459,8; V_4 = 473,6; V_5 = 500,2;$$

$$V_6 = 540,3; V_7 = 577,2; V_8 = 631,7; V_9 = 694,2; V_{10} = 737,9;$$

$$V_{11} = 764,4; V_{12} = 801,7; V_{13} = 859,3; V_{14} = 889,2; V_{15} = 916,1;$$

$$V_{16} = 963,2; V_{17} = 1011; V_{18} = 1053,3; V_{19} = 1121; V_{20} = 1212,9;$$

які представляють динаміку ВВП за $T = 20$ послідовних років, було побудовано та проведено верифікацію *лінійної прогностичної моделі*, а також побудовано «найкращу» *нелінійну* (а саме – *експоненціальну*) модель.

Зупинимось тепер детальніше на статистичних засобах оцінки *точності прогнозів*, які можна отримати з допомогою цих інструментів. При побудові *прогностичних моделей* в підрозділі 3.12 використовувались методи дослідження точність прогнозів *ex-post*. Тепер же звернемо увагу на «*прогнози ex-ante*», що стосуються *майбутніх*, а отже недоступних для спостереження значень прогнозованої змінної.

Подібне оцінювання вимагає знаходження *ймовірнісних розподілів* можливих помилок, а це, в свою чергу, вимагає залучення відповідних математичних інструментів теорії *ймовірностей та математичної статистики* [1], [2], [3], [6]. Питання аналізу точності *економетричного прогнозування* було предметом детального розгляду лабораторної роботи №3 (підрозділ 2.3). Оскільки *модель тенденції розвитку* – це частковий, спеці-

альний тип *економетричної* моделі, то використаємо цей матеріал та наведені там методи до аналізу точності «прогнозів *ex-ante*» для моделей, побудованих підрозділі 3.12.

1. Лінійна модель – статистичні припущення.

Припустимо, що часовий ряд V_1, V_2, \dots, V_T відображає динаміку зміни деякого кількісного показник явища, що вивчається, для послідовних моментів часу $t = 1, 2, \dots, T$.

Нехай V_τ – означає фактичне, але невідоме нам значення змінної V , а V_τ^* – відповідно прогноз цього значення, визначений за допомогою лінійної моделі *тенденції розвитку*.

Необхідно побудувати прогноз

$$\{V_\tau^*, \tau = T + 1, T + 2, \dots, T + S\}$$

майбутніх, а отже недоступних для спостереження значень

$$\{V_\tau, \tau = T + 1, T + 2, \dots, T + S\}$$

змінної V_t $t = 1, 2, \dots, .$

Нагадаємо (див. підрозділ 2.1), що згідно з визначенням, для того, щоб якість «судження» можна було вважати *статистичним прогнозом*, його *ймовірність* повинна бути *відомою* і достатньо *високою*.

На практиці цей принцип може мати різноманітні втілення. Наприклад з точки зору теорії ризику його можна сформулювати у вигляді наступної задачі:

- Для кожного часового інтервалу $\tau \in \{T + 1, T + 2, \dots, T + S\}$ заплановані межі «коридору» в якому *бажано* мати вартість V_τ .
- Задача полягає в тому, щоб для кожного з цих часових інтервалів:

$$\tau \in \{T + 1, T + 2, \dots, T + S\}$$

оцінити *ризик* (R_τ) того, що V_τ буде *за межами* встановленого «коридору» $[q_\tau^{(n)*}, q_\tau^{(e)*}]$, тобто необхідно знайти ймовірність наступних подій:

$$R_\tau = P\{V_\tau \notin [V_\tau^{(n)*}, V_\tau^{(e)*}]\}, \tau = T + 1, T + 2, \dots, T + S.$$

В теорії ризику подібні міри ризику отримали назву «*мір типу небезпеки*» (“*Downside risk measures*”).

Традиційний підхід *математичної статистики* до оцінки точності статистичних прогнозів полягає в побудові наряду з токовими прогнозами $\{V_\tau^*, \tau = T + 1, T + 2, \dots, T + S\}$ ще й *інтервального* прогнозу, або іншими словами «*інтервалів певності для прогнозованих значень*».

У випадку *класичної лінійної моделі тенденції розвитку*

$$V_t = b + a \cdot t + \xi_t, t = 1, 2, \dots,$$

її випадковий елемент ξ_t має наступні властивості:

- Розподіл ξ_t не залежить від t , $t = 1, 2, \dots, T$;
- ξ_t та ξ_s для різних t і s ($t \neq s$), незалежні та мають однаковий розподіл;
- Випадкова величина ξ_t має нормальний розподіл:

$$\xi_t \Leftrightarrow N(0; \sigma^2), t = 1, 2, \dots,$$

тобто

$$E(\xi_t) = 0, D(\xi_t) = \sigma^2, t = 1, 2, \dots$$

2. Помилка прогнозу (лінійна модель).

З метою оцінки точності прогнозування використовується помилка прогнозу, тобто число, що визначається рівністю:

$$e_\tau = V_\tau - V_\tau^*.$$

Якщо виконуються прийнятні відносно лінійної моделі тенденції розвитку припущення, то $e_\tau \in$ випадковою величиною, що має наступні параметри:

$$e_\tau \Leftrightarrow N(0; S^2(e_\tau)),$$

$$E(e_\tau) = 0; D(e_\tau) = S^2(e_\tau) = \sigma^2 \cdot \left[1 + \frac{1}{T} + \frac{(\tau - \bar{t})^2}{\sum_{t=1}^T (t - \bar{t})^2} \right].$$

При цьому $\tau \in \{T + 1, T + 2, \dots, T + S\}$, а $\bar{t} = \frac{1}{T} \sum_{t=1}^T t$.

Тому оцінкою «середнього» значення помилки прогнозу e_τ буде її стандартне відхилення:

$$|V_\tau - V_\tau^*| \approx S(e_\tau) = \sqrt{D(e_\tau)}, \tau \in \{T + 1, T + 2, \dots, T + S\}.$$

Замінюючи невідоме значення параметру σ^2 стохастичної структури моделі його незміщеною статистичною оцінкою σ^{*2} , отримаємо наступну формулу для оцінки $S^{*2}(e_\tau)$ дисперсії $S^2(e_\tau) = D(e_\tau)$ помилки прогнозу e_τ :

$$S^{*2}(e_\tau) = \sigma^{*2} \cdot \left[1 + \frac{1}{T} + \frac{(\tau - \bar{t})^2}{\sum_{t=1}^T (t - \bar{t})^2} \right].$$

3. Інтервал певності для прогнозованих значень.

Крім визначення точкового прогнозу V_τ^* змінної V , та дослідження його точності згідно з загальною процедурою економетричного прогнозування будуватиметься також інтервальний прогноз:

$$([d_{\tau}^*, g_{\tau}^*], \tau \in \{T+1, \dots, T+S\}).$$

Згідно з визначенням, *інтервальний прогноз* (або «прогнозований інтервал») – це числовий інтервал $[d_{\tau}^*, g_{\tau}^*]$, який з заданою наперед ймовірністю «покриває» точне (але невідоме) значення V змінної, що прогнозується.

Математична задача побудови інтервального прогнозу формулюється наступним чином.

- Припустимо, що задано близьке до 1 число β .
- Необхідно визначити числовий інтервал $[d_{\tau}^*, g_{\tau}^*]$ таким чином, щоб виконувалась рівність:

$$P\{d_{\tau}^* < V_{\tau} < g_{\tau}^*\} = \beta, \tau = T + s, s > 0,$$

де V_{τ} – фактичне, але невідоме нам значення змінної V в момент часу τ .

4. Оцінка точності (нормальний розподіл).

Припустимо, що значення параметру σ^2 стохастичної структури моделі відоме, а отже відомий також точний розподіл помилки прогнозу e_{τ} :

$$e_{\tau} = V_{\tau} - V_{\tau}^* \Leftrightarrow N(0; S^2(e_{\tau})).$$

Припустимо далі, що є можливість визначати будь-які *табличні значення*, пов'язані з довільним нормальним розподілом $N(m; \sigma^2)$ (використовуючи, наприклад, відповідну *статистичну функцію* аркушу «Excel», або процедуру пакету “Statystyka”).

Тоді практична процедура побудови *інтервального прогнозу* дуже проста.

- Вибираємо необхідне, близьке до 1 число β ;
- Використовуючи відповідні таблиці, визначаємо δ_{β} з умови:

$$P\{N(0; S^2(e_{\tau})) < \delta_{\beta}\} = \frac{1 + \beta}{2}, \tau = T + s, s > 0.$$

Це буде означати, що

$$P\{-\delta_{\beta} < N(0; S^2(e_{\tau})) < \delta_{\beta}\} = \beta, \tau = T + s, s > 0.$$

Тобто:

$$P\{-\delta_{\beta} < e_{\tau} < \delta_{\beta}\} = \beta, \tau = T + s, s > 0,$$

або

$$P\{V_{\tau}^* - \delta_{\beta} < y_{\tau} < V_{\tau}^* + \delta_{\beta}\} = \beta, \tau = n + s, s > 0.$$

Отже межі $[d_{\tau}^*, g_{\tau}^*]$ *інтервального прогнозу* визначаються рівностями:

$$d_{\tau}^* = y_{\tau}^* - \delta_{\beta}; g_{\tau}^* = y_{\tau}^* + \delta_{\beta},$$

$$\tau = n + s, s > 0.$$

Однак відповідних друкованих таблиць для нормального розподілу $N(m; \sigma^2)$ з довільними параметрами ($m; \sigma^2$) не існує.

Щільність $f_{\xi}(x)$ випадкової величини ξ , яка має нормальний розподіл з параметрами (m, σ^2), визначається формулою:

$$f_{\xi}(x) = \frac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{(x-m)^2}{2\sigma^2}}, \quad -\infty < x < \infty;$$

Математичне сподівання та дисперсія нормального розподілу з параметрами (m, σ^2), відповідно дорівнюють:

$$m = E(\xi); \quad \sigma^2 = D(\xi).$$

Укладання детальних таблиць подібних розподілів – дуже трудомістка та коштовна процедура. Але в цьому немає необхідності.

➤ У випадку нормального розподілу цілком вистачить однієї таблиці, для будь-якого одного конкретного набору параметрів.

Такий «конкретний набір» – це параметри (0, 1).

➤ Нормальний розподіл з параметрами (0, 1) називається *стандартним нормальним розподілом*.

Відповідну випадкову величину будемо позначати символом η :

$$\eta \Leftrightarrow N(0, 1)$$

Для стандартного нормального розподілу випадку, коли $m = 0$ та $\sigma^2 = 1$, щільність $f_{\eta}(x)$ приймає вигляд:

$$f_{\eta}(x) = \frac{1}{\sqrt{2\pi}} \cdot e^{-\frac{x^2}{2}}, \quad -\infty < x < \infty.$$

- Функція розподілу стандартного нормального розподілу: $\eta \Leftrightarrow N(0, 1)$ називається *функцією Лапласа* та визначається формулою:

$$\Phi(x) = P\{\eta < x\} = P\{N(0, 1) < x\} = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^x e^{-\frac{u^2}{2}} du, \quad -\infty < x < \infty,$$

Пригадаємо ще одну властивість нормального розподілу:

➤ Якщо випадкова величина ξ має нормальний розподіл з параметрами (m, σ^2): $\xi \Leftrightarrow N(m, \sigma^2)$, то випадкова величина:

$$\eta = \frac{\xi - m}{\sigma}$$

буде мати нормальний стандартний розподіл: $\eta \Leftrightarrow N(0, 1)$

Функція Лапласа, з свого боку, відзначається такими властивостями:

$$\Phi(0) = 0,5; \quad \Phi(-a) = 1 - \Phi(a).$$

Пригадаємо також, число u_α , яке визначається рівністю:

$$P\{N(0, 1) < u_\alpha\} = \Phi(u_\alpha) = \alpha.$$

називається «квантилем порядку α » для стандартного нормального розподілу.

Оскільки решта e_τ розподілена за нормальним законом з параметрами $(0; S^2(e_\tau))$: $e_\tau \Leftrightarrow N(0; S^2(e_\tau))$, то підставі приведені властивості:

$$\frac{N(0, S^2(e_\tau))}{\sqrt{S^2(e_\tau)}} \Leftrightarrow N(0; 1).$$

Тобто:

$$\frac{e_\tau}{\sqrt{S^2(e_\tau)}} \Leftrightarrow N(0; 1).$$

Знайдемо коефіцієнт z_β з умови:

$$P\{-z_\beta < N(0; 1) < z_\beta\} = \beta.$$

Очевидно, що z_β – це квантиль порядку $\frac{1+\beta}{2}$ для стандартного нормального розподілу $z_\beta = u_{\frac{1+\beta}{2}}$: $P\{N(0; 1) < z_\beta\} = \Phi(z_\beta) = \frac{1+\beta}{2} = \Phi\left(u_{\frac{1+\beta}{2}}\right)$.

Тоді:

$$P\left\{-z_\beta < \frac{e_\tau}{\sqrt{S^2(e_\tau)}} < z_\beta\right\} = \beta.$$

Тобто:

$$P\left\{-z_\beta < \frac{V_\tau - V_\tau^*}{\sqrt{S^2(e_\tau)}} < z_\beta\right\} = \beta.$$

Або рівнозначно:

$$P\{V_\tau^* - z_\beta \cdot \sqrt{S^2(e_\tau)} < V_\tau < V_\tau^* + z_\beta \cdot \sqrt{S^2(e_\tau)}\} = \beta, \tau > T.$$

А це значає, що числовий інтервал:

$$[d_\tau^* = V_\tau^* - z_\beta \cdot \sqrt{S^2(e_\tau)}; g_\tau^* = V_\tau^* + z_\beta \cdot \sqrt{S^2(e_\tau)}]$$

визначає інтервальний прогноз для значення y_τ , $\tau > n$ змінної Y .

5. Прогнозований інтервал на підставі t -розподілу.

На практиці значення параметру σ^2 є невідомим, а отже скористатися нормальним розподілом можна тільки у випадку, якщо йдеться про *наближений* розв'язок задачі побудови прогнозованого інтервалу. Для цього необхідно:

- Замінити невідоме значення параметру σ^2 незміщеною статистичною оцінкою σ^{*2} у формулі для дисперсії $S^2(e_\tau) = D(e_\tau)$ помилки прогнозу.

Отримаємо наступну формулу для оцінки $S^{*2}(e_\tau)$ дисперсії $S^2(e_\tau)$

$$\text{помилки прогнозу } e_\tau: S^{*2}(e_\tau) = \sigma^{*2} \cdot \left[1 + \frac{1}{T} + \frac{(\tau - \bar{t})^2}{\sum_{t=1}^T (t - \bar{t})^2} \right].$$

Якщо хочемо точніше оцінити результати прогнозування, і при цьому виконуються прийняті відносно моделі припущення, то можна скористатися результатами з області *статистичного оцінювання*.

- Якщо виконуються прийняті щодо моделі припущення, то статистика:

$$\frac{e_\tau}{\sqrt{S^{*2}(e_\tau)}} = \frac{V_\tau - V_\tau^*}{\sqrt{S^{*2}(e_\tau)}} \Leftrightarrow t_{(n-2)}, \tau = T + s, s > 0,$$

буде мати розподіл t -Стюдента з $(n - 2)$ степенями свободи.

Отже практична процедура побудови *інтервального прогнозу* буде виглядати наступним чином:

- Вибираємо необхідне, близьке до 1 число;

Нехай $S_{(n)}(x)$ позначає функцію розподіл випадкової величини $t_{(n)}$,

$$S_{(n)}(x) = P\{t_{(n)} < x\}, -\infty < x < \infty,$$

яка має t -розподіл Стюдента з (n) степенями свободи.

- Використовуючи відповідні таблиці, визначаємо величину δ_β з умови:

$$P\{t_{(n-2)} < t_\beta\} = S_{(n-2)}(t_\beta) = \frac{1 + \beta}{2}.$$

Це буде означати, що $P\{-t_\beta < t_{(n-2)} < t_\beta\} = \beta$.

Тобто:

$$P\left\{-t_\beta < \frac{V_\tau - V_\tau^*}{\sqrt{S^{*2}(e_\tau)}} < t_\beta\right\} = \beta, \tau = T + s, s > 0.$$

Або рівнозначно:

$$P\{V_\tau^* - t_\beta \cdot \sqrt{S^{*2}(e_\tau)} < V_\tau < V_\tau^* + t_\beta \cdot \sqrt{S^{*2}(e_\tau)}\}, \tau = T + s, s > 0.$$

А це означає, що числовий інтервал:

$$[d_\tau^* = V_\tau^* - t_\beta \cdot \sqrt{S^{*2}(e_\tau)}; g_\tau^* = V_\tau^* + t_\beta \cdot \sqrt{S^{*2}(e_\tau)}]$$

визначає *інтервальний прогноз* для значення V_τ , $\tau > T$ змінної V .

- Отже межі $[d_\tau^*, g_\tau^*]$ *інтервального прогнозу* дорівнюють:

$$d_\tau^* = V_\tau^* - t_\beta \cdot \sqrt{S^{*2}(e_\tau)}; g_\tau^* = V_\tau^* + t_\beta \cdot \sqrt{S^{*2}(e_\tau)}, \tau = T + s, s > 0.$$

4.14. Прогноз динаміки національного доходу: прикладі та завдання для самоконтролю.

1. Прогнозування в моделях тенденції розвитку. 2. Вибір аналітичної форми моделі тенденції розвитку. 3. Лінійна трансформація експоненціальної моделі. 4. Побудова нелінійної прогностичної моделі. 5. Лінія регресії нелінійної моделі (історичний прогноз).

1. Прогнозування в моделях тенденції розвитку.

Числові дані

$$V_1 = 764,4; V_2 = 801,7; V_3 = 859,3; V_4 = 889,2; V_5 = 916,1;$$

$$V_6 = 963,2; V_7 = 1011; V_8 = 1053,3; V_9 = 1121; V_{10} = 1212,9;$$

представляють динаміку ВВП за $T = 10$ послідовних років.

➤ Спираючись на них необхідно визначити прогноз значення ВВП на наступні два роки та оцінити *точність* такого прогнозування.

Тобто дати *кількісну оцінку ризиків*, пов'язаних з таким прогнозом. З цією метою використати описаний в підрозділі 3.11 «метод лінійної трансформації», а саме:

➤ Знайти аналітичний вигляд функції тренду $f(t)$, $t = 1, 2, \dots, T$, яка «найкраще» описує динаміку емпіричних даних $\{V_1, V_2, \dots, V_T\}$, представлених часовим рядом.

З цією метою необхідно:

- Сформулювати множину *робочих гіпотез* щодо функції $f(t)$:

$$\{f_1(t), f_2(t), \dots, f_k(t)\}.$$

- Для кожної гіпотетичної функції $f_i(t)$, $i = 1, 2, \dots, k$, знайти значення

$$R_i^{*2}, i = 1, 2, \dots, k,$$

множника детермінації.

➤ «Найкраще» динаміку емпіричних даних $\{V_1, V_2, V_3, \dots, V_T\}$ описує функція, для якої значення множника детермінації R_i^{*2} є *найбільшим*.

➤ Якщо «найкраща» модель не є лінійною, то виконуємо її *лінійну трансформацію*:

$$V_t \rightarrow Z_t.$$

Тобто проводимо перетворення емпіричних даних:

$$\{V_1, V_2, \dots, V_T\} \rightarrow \{Z_1, Z_2, \dots, Z_T\},$$

що містяться у векторі $\{V_1, V_2, \dots, V_T\}$, таким чином:

$$\{(t, V_t), t = 1, 2, \dots, T\} \rightarrow \{(u, Z_t), t = 1, 2, \dots, T\},$$

щоб звести нелінійну модель $f_i(t)$ до лінійної:

$$z_i(u) = B_i + A_i u, u = 1, 2, \dots, T.$$

- Спочатку визначаємо *точковий* та *інтервальний* прогнози, використовуючи лінійну модель.

$$z_i(u) = B_i + A_i u, u = 1, 2, \dots, T.$$

$$\{(u, Z_t), t = 1, 2, \dots, T\},$$

- Остаточні *точковий* та *інтервальний* прогнози для *нелінійної* моделі обчислюємо на підставі відповідних лінійних прогнозів, перетворюючи їх згідно з формулами *лінійної трансформації* вибраної *нелінійної* функції тенденції розвитку.

2. Вибір аналітичної форми моделі тенденції розвитку.

Побудувати в аркуші «Excel» графік точок $\{(1, V_1), (2, V_2), \dots, (n, V_n)\}$, що представляють *числові дані моделі* $\{(t, V_t), t = 1, 2, \dots, 10\}$.

Провести візуальний аналіз графіка та сформулювати робочі гіпотези. Функцію, яка «найкраще описує» емпіричні дані $\{V_1, V_2, V_3, \dots, V_T\}$, вибрати серед наступних моделей:

- *Лінійна* $V_t = b + a \cdot t, t = 1, 2, \dots$;
- *Степенева* $V_t = b \cdot t^a, t = 1, 2, \dots$;
- *Експоненціальна* $V_t = b \cdot a^t, t = 1, 2, \dots$;
- *Логарифмічна* $V_t = b + a \cdot \ln(t), t = 1, 2, \dots$.

Використовуючи опцію «Формат лінії тренду» аркушу «Excel», додати до збудованого графіка *теоретичну модель* для кожної гіпотетичної функції $f_i(t)$.

Використати опцію:

- «Помістити на діаграму величину достовірності апроксимації R^2 » та знайти для кожної гіпотетичної функції $f_i(t)$ значення R_i^{*2} множника детермінації.
- «Найкраще» динаміку емпіричних даних $\{V_1, V_2, V_3, \dots, V_T\}$ описує функція, для якої значення множника детермінації R_i^{*2} є *найбільшим*.

Відповідь: *Лінійна:* $R_1^{*2} \approx 0,9777$. Модель пояснює 98% зміни V .

Степенева: $R_2^{*2} \approx 0,8842$. Модель пояснює 88% зміни V .

Експоненціальна: $R_3^{*2} \approx 0,9904$. Модель пояснює 99% зміни V .

Логарифмічна: $R_4^{*2} \approx 0,838$. Модель пояснює 84% зміни V .

«Найточніше» емпіричні дані описує *експоненціальна* модель.

3. Лінійна трансформація експоненціальної моделі.

«Найточніше» динаміку емпіричних даних, представлених часовим рядом $\{V_1, V_2, V_3, \dots, V_T\}$ описує функція:

$$V_t = b \cdot a^t + \zeta_t, t = 1, 2, \dots,$$

або

$$V_t = b \cdot e^{c \cdot t} + \zeta_t, t = 1, 2, \dots, (c = \ln(a)).$$

Проведемо *лінійну трансформацію* експоненціальної моделі тенденції розвитку. Тобто виконаємо перетворення емпіричних даних, що містяться у векторі $\{V_1, V_2, \dots, V_n\}$, таким чином, щоб звести нелінійну (*експоненціальну*) модель до лінійної:

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots$$

Розв'язок. Лінійна трансформація моделі має вигляд:

$$Z_t = \ln(V_t), t = 1, 2, \dots, T.$$

Модель

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots, .$$

Параметри:

$$B = \ln(b); A = \ln(a).$$

Відповідні емпіричні дані моделі:

$$\{(1, Z_1), (2, Z_2), \dots, (n, Z_n)\} = \{(t, Z_t), t = 1, 2, \dots, 10\}.$$

Відповідь: $Z_1 \approx 6,639; Z_2 \approx 6,687; Z_3 \approx 6,756; Z_4 \approx 6,790; Z_5 \approx 6,820;$
 $Z_6 \approx 6,870; Z_7 \approx 6,919; Z_8 \approx 6,96; Z_9 \approx 7,022; Z_{10} \approx 7,101.$

Застосовуючи класичний метод найменших квадратів до моделі:

$$Z_t = B + A \cdot t + \xi_t, t = 1, 2, \dots, .$$

використовуючи *перетворені емпіричні дані*:

$$\{(t, Z_t), t = 1, 2, \dots, 10\},$$

знайти за допомогою функції „ЛНІЙН” аркушу «Excel» наступні величини:

- Значення $\{B^*, A^*\}$ оцінок МНК параметрів A і B .
Відповідь: $A^* = 0,048; B^* = 6,591.$
- Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури моделі.
Відповідь: $\sigma^2 \approx \sigma^{*2} \approx 0,00023; \sigma \approx \sigma^* \approx 0,0153.$
- Значення R^{*2} множника детермінації.
Відповідь: $R^{*2} \approx 0,99038.$

4. Побудова нелінійної прогностичної моделі.

Використовуючи «метод лінійної трансформації» знайти оцінки (a^*, b^*) параметрів a і b початкової нелінійної моделі.

Розв'язок. Оцінки (a^*, b^*) параметрів a і b початкової нелінійної моделі обчислюємо на підставі оцінок B^* і A^* параметрів A і B трансформованої моделі за формулами:

$$b^* = \exp(B^*) = e^{B^*}; a^* = \exp(A^*) = e^{A^*}; c^* = \ln(a^*) = A^*.$$

Відповідь: $a^* = 1,0494; b^* = 728,666;$
або $c^* = 0,0482; b^* = 728,666.$

5. Лінія регресії нелінійної моделі (історичний прогноз).

Використовуючи побудовану нелінійну модель тенденції розвитку побудувати лінію регресії моделі, тобто обчислити теоретичні значення

$$\{(t, V_t^*), t = 1, 2, \dots, T\} \text{ моделі: } V_t^* = b^* \cdot (a^*)^t, t = 1, 2, \dots, T.$$

Відповідь: $V_1^* \approx 764,66$; $V_2^* \approx 802,43$; $V_3^* \approx 842,06$; $V_4^* \approx 883,65$; $V_5^* \approx 927,295$; $V_6^* \approx 973,097$; $V_7^* \approx 1021,16$; $V_8^* \approx 1071,60$; $V_9^* \approx 1124,53$; $V_{10}^* \approx 1180,07$.

Побудувати в аркуші «*Excel*» графік точок:

$$\{(1, V_1), (2, V_2), \dots, (T, V_T)\},$$

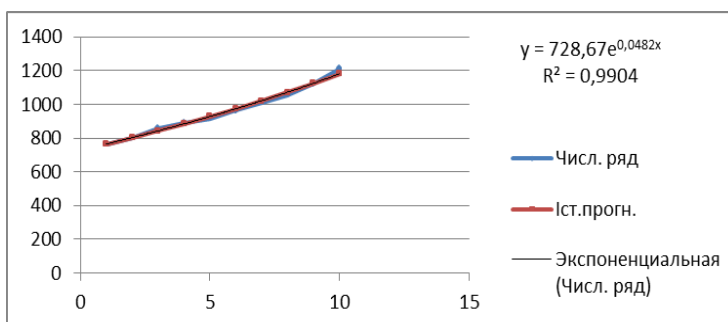
що представляють числові дані $\{(t, V_t), t = 1, 2, \dots, 10\}$ початкової моделі.

Додати до побудованого графіку лінію «історичного прогнозу»:

$$\{(1, V_1^*), (2, V_2^*), \dots, (T, V_T^*)\}.$$

Використовуючи графік емпіричних даних $\{(t, V_t), t = 1, 2, \dots, 10\}$ та застосовуючи опцію «*Формат лінії тренду*» аркушу «*Excel*» виконати наступні завдання:

- Додати до збудованого графіка *теоретичну модель*;
- Знайти *статистичні оцінки* (a^* , b^*) для структурних параметрів нелінійної моделі;
- Знайти числове значення (R^{*2}) множника детермінації R^2 .



Використовуючи емпіричні дані моделі $\{(1, V_1), (2, V_2), \dots, (n, V_n)\}$, і застосовуючи функцію «*ЛГРФНАБЛ*» аркушу «*Excel*», знайти:

- Значення $\{a^*, b^*\}$ оцінок МНК для структурних параметрів моделі.
- Значення $\{S^*(a), S^*(b)\}$ стандартних відхилень цих оцінок.
- Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури моделі.
- Значення R^{*2} множника детермінації.

Відповідь: Функція «*ЛГРФНАБЛ*»

a^*	1,0494	728,666	b^*
$S^*(a)$	0,00168	0,0104	$S^*(b)$
R^{*2}	0,99038	0,0153	σ^*

4.15. Надійність економетричного прогнозу.

1. Лінійна модель (нормальний розподіл). 2. Економетричний прогноз на основі нелінійної моделі. 3. Оцінка точності з допомогою *t*-розподілу Стьюдента.

Застосовуючи «метод лінійної трансформації», визначаємо спочатку *точковий* та *інтервальний* прогнози, використовуючи *трансформовану* лінійну модель. Остаточні *точковий* та *інтервальний* прогнози для заданого часового ряду обчислюємо на підставі відповідних *лінійних прогнозів*, перетворюючи їх згідно з формулами *лінійної трансформації* нелінійних моделей.

1. Лінійна модель (нормальний розподіл).

Використовуючи побудовану лінійну модель тенденції розвитку:

$$Z^*_t = B^* + A^* \cdot t, \quad t = 1, 2, \dots,$$

визначити *точковий* прогноз

$$\{(\tau, Z^*_\tau), \tau = 11, 12\}$$

для *трансформованої* змінної Z_t .

Відповідь: $Z^*_{11} \approx 7,1215$; $Z^*_{12} \approx 7,1698$.

Оцінка точності з допомогою нормального розподілу.

Вибрати «*надійність*» (β) точності прогнозу рівною: $\beta = 0,9$.

Оцінити *точність* *точкового* прогнозу $\{(\tau, Z^*_\tau), \tau = 11, 12\}$, тобто знайти *приблизне* значення різниці:

$$|Z_\tau - Z^*_\tau|, \quad (\tau = 11, 12).$$

Помилка прогнозу $e_\tau = Z_\tau - Z^*_\tau$ для лінійної моделі тенденції розвитку має нормальний розподіл: $e_\tau = Z_\tau - Z^*_\tau \Leftrightarrow N(0; S^2(e_\tau))$, де

$$E(e_\tau) = 0; \quad D(e_\tau) = S^2(e_\tau) = \sigma^2 \cdot \left[1 + \frac{1}{T} + \frac{(\tau - \bar{t})^2}{\sum_{t=1}^T (t - \bar{t})^2} \right]; \quad \bar{t} = \frac{1}{T} \sum_{t=1}^T t.$$

Значення σ^{*2} незміщеної статистичної оцінки $\hat{\sigma}^2$ для параметру σ^2 стохастичної структури лінійної моделі:

Відповідь: $\sigma^{*2} \approx 0,00023$.

Замінюючи невідоме значення параметру σ^2 стохастичної структури лінійної моделі його незміщеною статистичною оцінкою σ^{*2} , отримуємо *наближену* оцінку $S^{*2}(e_\tau)$ дисперсії $S^2(e_\tau)$ помилки прогнозу e_τ :

Відповідь: $S^{*2}(e_{11}) \approx 0,00034$; $S^*(e_{11}) \approx 0,0185$;
 $S^{*2}(e_{12}) \approx 0,00038$; $S^*(e_{12}) \approx 0,0194$.

Застосовуючи функцію «НОРМ. ОБЕР» аркушу «Excel» визначити для вибраного «рівня надійність» $\beta = 0,9$ величину δ_β з умови:

$$P\{N(0; S^2(e_\tau)) < \delta_\beta(\tau)\} = \frac{1+\beta}{2}, (\tau = 11, 12).$$

Відповідь: $\delta_\beta(\tau_{11}) = 0,0304$; $\delta_\beta(\tau_{12}) = 0,0319$.

Використовуючи визначений *точковий* прогноз:

$$\{(\tau, Z_\tau^*), \tau = 11, 12\}$$

побудувати для кожного моменту часу ($\tau = 11, 12$) *інтервальний прогноз*

$$[D_\tau^*, G_\tau^*],$$

для *трансформованої* змінної Z_τ , при умові, що ймовірність β рівна:

$$\beta = 0,9:$$

Розв'язок. Межі *інтервального прогнозу* обчислюємо за формулами:

$$D_\tau^* = Z_\tau^* - \delta_\beta; G_\tau^* = Z_\tau^* + \delta_\beta, \tau > T.$$

Відповідь: $D_{11}^* = 7,0911$; $G_{11}^* = 7,1519$; $D_{12}^* = 7,1379$; $G_{12}^* = 7,2016$.

Використання функції Лапласа.

Визначити для вибраного «рівня надійність» $\beta = 0,9$ коефіцієнт z_β з умови:

$$P\{-z_\beta < N(0; 1) < z_\beta\} = \beta.$$

Якщо

$$\Phi(x) = P\{\eta < x\} = P\{N(0, 1) < x\},$$

означає функцію Лапласа, то коефіцієнт z_β знаходимо з рівності:

$$\Phi(z_\beta) = \frac{1+\beta}{2}.$$

Відповідь: $z_\beta = 1,645$.

Використовуючи визначений *точковий* прогноз (τ, Z_τ^*), побудувати для кожного моменту часу ($\tau = 11, 12$) *інтервальні прогнози*:

$$[D_\tau^*, G_\tau^*],$$

для *трансформованої* змінної Z_τ , при умові, що ймовірність β рівна:

$$\beta = 0,9:$$

Розв'язок. Межі *інтервального прогнозу* обчислюємо за формулами:

$$D_\tau^* = Z_\tau^* - z_\beta \cdot S^*(e_\tau); G_\tau^* = Z_\tau^* + z_\beta \cdot S^*(e_\tau), \tau > T.$$

Відповідь: $D_{11}^* = 7,0911$; $G_{11}^* = 7,1519$; $D_{12}^* = 7,1379$; $G_{12}^* = 7,2016$.

2. Економетричний прогноз на основі нелінійної моделі.

Використовуючи визначений *точковий* прогноз $\{(\tau, Z_\tau^*), \tau = 11, 12\}$ та побудований *інтервальний прогноз* $[D_\tau^*, G_\tau^*]$, для кожного моменту часу ($\tau = 11, 12$) для *трансформованої* змінної Z_τ , при умові, що ймовірність β рівна: $\beta = 0,9$, побудувати відповідні *точкові*

$$\{(\tau, V^*_\tau), \tau = 11, 12\},$$

та інтервальні

$$\{(\tau, [d^*_\tau, g^*_\tau]), \tau = 11, 12\},$$

прогнози для нелінійної моделі.

Розв'язок. Точкові прогнози

$$\{(\tau, V^*_\tau), \tau = 11, 12\}$$

для змінної V_t , яка представляє динаміку величини ВВП, обчислюємо на підставі точкового прогнозу

$$\{(\tau, Z^*_\tau), \tau = 11, 12\}$$

трансформованої змінної Z_t , за формулами:

$$V^*_\tau = \exp(Z^*_\tau), \tau = 11, 12.$$

Інтервальні прогнози $\{[d^*_\tau, g^*_\tau], \tau = 11, 12\}$ для змінної V_t обчислюємо на підставі інтервального прогнозу

$$\{[D^*_\tau, G^*_\tau], \tau = 11, 12\}$$

трансформованої змінної Z_t , за формулами:

$$d^*_\tau = \exp(D^*_\tau), g^*_\tau = \exp(G^*_\tau), \tau = 11, 12.$$

$$\text{Відповідь: } (V^*_{11} = 1238,36; d_{11}^* = 1201,36; g_{11}^* = 1276,57); \\ (V^*_{12} = 1299,52; d_{12}^* = 1258,76; g_{12}^* = 1341,6).$$

3. Оцінка точності з допомогою t -розподілу Стьюдента.

Визначити для вибраного «рівня надійності» $\beta = 0,9$ коефіцієнт t_β з умови:

$$P\{-t_\beta < t_{(n-2)} < t_\beta\} = \beta.$$

Якщо

$$S_{(n)}(x) = P\{t_{(n)} < x\}, -\infty < x < \infty,$$

функція розподіл випадкової величини $t_{(n)}$, що має t -розподіл Стьюдента з n степенями свободи, то коефіцієнт t_β знаходимо з рівняння:

$$S_{(n-2)}(t_\beta) = \frac{1 + \beta}{2}.$$

Використовуючи функцію „СТЮДЕНТ.ОБЕР” аркушу «Excel», знайти коефіцієнт t_β .

$$\text{Відповідь: } t_\beta = 1,8595.$$

Економетричний прогноз на основі лінійної моделі.

Використовуючи визначений точковий прогноз (τ, Z^*_τ) , побудувати для кожного моменту часу ($\tau = 11, 12$) інтервальний прогноз $[D^*_\tau, G^*_\tau]$, для трансформованої змінної Z_t , при умові, що ймовірність β рівна:

$$\beta = 0,9:$$

Розв'язок. Задача побудови інтервального прогнозу формулюється наступним чином:

➤ Необхідно визначити числовий інтервал $[D_\tau^*, G_\tau^*]$ таким чином, щоб виконувалась рівність:

$$P\{D_\tau^* < Z_\tau < G_\tau^*\} = \beta, \tau = T + s, s > 0.$$

При використанні t -розподілу Стюдента межі інтервалу $[D_\tau^*, G_\tau^*]$ лінійної моделі визначаються за формулами:

$$D_\tau^* = Z_\tau^* - t_\beta \cdot S^*(e_\tau), G_\tau^* = Z_\tau^* + t_\beta \cdot S^*(e_\tau), \tau > T.$$

Відповідь: $(D_{11}^* = 7,0871; G_{11}^* = 7,1559); (D_{12}^* = 7,1337; G_{12}^* = 7,2058)$.

Економетричний прогноз на основі нелінійної моделі.

Використовуючи визначений *точковий* прогноз $\{(\tau, Z_\tau^*), \tau = 11, 12\}$ та побудований *інтервальний* прогноз $[D_\tau^*, G_\tau^*]$, для кожного моменту часу $(\tau = 11, 12)$ для *трансформованої* змінної Z_τ , при умові, що надійність прогнозу рівна: $\beta = 0,9$, побудувати відповідні *точкові* $\{(\tau, V_\tau^*), \tau = 11, 12\}$, та *інтервальні* $\{(\tau, [d_\tau^*, g_\tau^*]), \tau = 11, 12\}$, прогнози для нелінійної моделі.

Точкові прогнози $\{(\tau, V_\tau^*), \tau = 11, 12\}$ для змінної V_τ , обчислюємо на підставі *точкового* прогнозу $\{(\tau, Z_\tau^*), \tau = 11, 12\}$ трансформованої змінної Z_τ , за формулами:

$$V_\tau^* = \exp(Z_\tau^*), \tau = 11, 12.$$

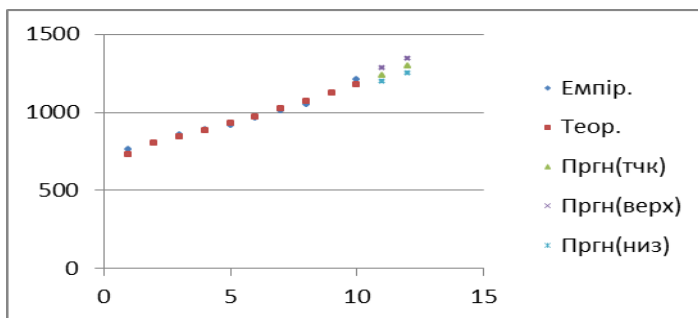
Відповідь: $V_{11}^* = 1238,36; V_{12}^* = 1299,52$.

Інтервальні прогнози $\{[d_\tau^*, g_\tau^*], \tau = 11, 12\}$ для змінної V_τ обчислюємо на підставі *інтервального* прогнозу $\{[D_\tau^*, G_\tau^*], \tau = 11, 12\}$ трансформованої змінної Z_τ , за формулами:

$$d_\tau^* = \exp(D_\tau^*), g_\tau^* = \exp(G_\tau^*), \tau = 11, 12.$$

Відповідь: $(d_{11}^* = 1196,53; g_{11}^* = 1281,65); (d_{12}^* = 1253,54; g_{12}^* = 1347,19)$.

Дати графічну ілюстрацію процедури економетричного прогнозування на основі нелінійної моделі тенденції розвитку, реалізованої в попередніх завданнях.



4.16. Точність прогнозів методу «повзучого тренду»: прикладі та завдання для самоконтролю.

1. Точковий прогноз «*ex-ante*».
2. Обчислення інтервальних прогнозів.
3. Оцінка точності з допомогою нормального розподілу.
4. Використання функції Лапласа.
5. Графічна ілюстрація результатів.

Продовжимо розпочатий в підрозділі 4.5 аналіз наступного часового ряду:

$$y_1 = 26; y_2 = 25; y_3 = 31; y_4 = 23; y_5 = 32; y_6 = 31; \\ y_7 = 33; y_8 = 28; y_9 = 31; y_{10} = 33; y_{11} = 25; y_{12} = 27.$$

який відображає попит протягом року на певний товар.

На підставі цього ряду необхідно було виконати *оперативне прогнозування* можливих його чергових значень $\{y^*_{13}, y^*_{14}, y^*_{15}\}$.

Проведені в підрозділі 4.10 дослідження дозволили вибрати «найкраще» серед кількох можливих значення для сталої згладжування методу «повзучого тренду»: $k = 3$.

Скористаємось цим, побудуємо та проаналізуємо *якість* коротко-строкових «прогнозів *ex-ante*» для невідомих значень $\{y_{13}, y_{14}, y_{15}\}$ прогнозованої змінної Y в наступному кварталі.

1. Точковий прогноз «*ex-ante*».

Завдання 1. Провести «згладжування» всіх доступних спостережень

$$y_1, y_2, \dots, y_t,$$

часового ряду за допомогою методу «повзучого тренду» зі сталою згладжування $k = 3$. З цією метою:

- 1) Поділити часовий ряд y_1, y_2, \dots, y_n на послідовні відрізки довжини 3:

$$(y_1, y_2, y_3); (y_2, y_3, y_4); \dots; (y_{10}, y_{11}, y_{12}).$$

- 2) Використовуючи функцію «ЛІНІЙНА» аркушу «Excel» побудувати відповідні функції лінійних трендів $f_i(t)$ для непарних значень $i = 1, 3, 5, \dots$:

$$f_1(t) = b_1 + a_1 t, t = 1, 2, 3;$$

$$f_3(t) = b_3 + a_3 t, t = 3, 4, 5; \dots,$$

...

$$f_9(t) = b_9 + a_9 t, t = 9, 10, 11.$$

Відповідь. $(b_1, a_1) = (2,5, 22,3); (b_3, a_3) = (0,5, 26,7);$

$(b_5, a_5) = (0,5, 29); (b_7, a_7) = (-1, 38,7); (b_9, a_9) = (-3, 59,7).$

- 3) Використовуючи побудовані функції трендів $f_i(t)$ для непарних значень $i = 1, 3, 5, 7, 9$, обчислити відповідні теоретичні значення:

$$((\hat{y}_1^{(1)} = f_1(1), \hat{y}_2^{(1)} = f_1(2), \hat{y}_3^{(1)} = f_1(3));$$

$$(\hat{y}_3^{(3)} = f_3(3), \hat{y}_4^{(3)} = f_3(4), \hat{y}_5^{(3)} = f_3(5));$$

...

$$(\hat{y}_9^{(9)} = f_9(9), \hat{y}_{10}^{(9)} = f_9(10), \hat{y}_{11}^{(9)} = f_9(11)).$$

4) Використовуючи функцію «ТЕНДЕНЦІЯ» аркушу «Excel» обчислити відповідні теоретичні значення функції трендів $f_i(t)$ для парних значень i :

$$((\hat{y}_2^{(2)} = f_2(2), \hat{y}_3^{(2)} = f_2(3), \hat{y}_4^{(2)} = f_2(4));$$

$$(\hat{y}_4^{(4)} = f_4(4), \hat{y}_5^{(4)} = f_4(5), \hat{y}_6^{(4)} = f_4(6));$$

...;

$$(\hat{y}_{10}^{(10)} = f_{10}(10), \hat{y}_{11}^{(10)} = f_{10}(11), \hat{y}_{12}^{(10)} = f_{10}(12)).$$

5) Використовуючи функцію «СЕРЕДНС» аркушу «Excel» обчислити для кожного елементу (y_t) часового ряду відповідні їм згладжені значення (y_t^*).

Застосований принцип «повзучого тренду» створює ситуацію, коли деякі значення y_t часового ряду можуть бути спільними одночасно для кількох сегментів згладжування.

Відповідь: $y_1^* = 24,83$; $y_2^* = 27,3$; $y_3^* = 28,1$; $y_4^* = 26,2$; $y_5^* = 29,78$;
 $y_6^* = 32,28$; $y_7^* = 31,61$; $y_8^* = 29,33$; $y_9^* = 31$; $y_{10}^* = 31,39$; $y_{11}^* = 27,5$; $y_{12}^* = 25,33$.

Завдання 2. Обчислити для послідовних періодів часу $t = 2, 3, \dots, 12$, прирости $\{w_t^*, t = 2, 3, \dots, 12\}$ «згладженого» за допомогою повзучого тренду часового ряду y_1, y_2, \dots, y_{12} , за формулою:

$$w_t^* = y_t^* - y_{t-1}^*, t = 2, 3, \dots, 12.$$

Відповідь: $w_2^* = 2,5$; $w_3^* = 0,78$; $w_4^* = -1,89$; $w_5^* = 3,56$; $w_6^* = 2,5$;
 $w_7^* = -0,67$; $w_8^* = -2,28$; $w_9^* = 1,67$; $w_{10}^* = 0,39$; $w_{11}^* = -3,89$; $w_{12}^* = -2,17$.

Завдання 3. Визначити послідовні значення гармонічних ваг:

$$H_1^{12}, H_2^{12}, \dots, H_{12}^{12}.$$

Для цього скористатися наступним алгоритмом:

$$H_1^{12} = 0;$$

$$H_{t+1}^{12} = H_t^{12} + \frac{1}{11 \cdot (12 - t)}, t = 1, 2, \dots, 11.$$

Відповідь: $H_1^{12} = 0$; $H_2^{12} = 0,0082$; $H_3^{12} = 0,0174$;
 $H_4^{12} = 0,0274$; $H_5^{12} = 0,0388$; $H_6^{12} = 0,0518$; $H_7^{12} = 0,067$; $H_8^{12} = 0,0851$;
 $H_9^{12} = 0,1079$; $H_{10}^{12} = 0,1382$; $H_{11}^{12} = 0,1836$; $H_{12}^{12} = 0,2745$.

Завдання 4. Використовуючи гармонічні ваги $H_1^{12}, H_2^{12}, \dots, H_{12}^{12}$, та прирости $\{w_t^*, t = 2, 3, \dots, 12\}$ «згладженого» часового ряду, визначити прогноз $w_{13,p}$ можливого приросту w_{13} в момент $t = 13$ за формулою:

$$w_{13,p} = w_2^* \cdot H_2^{12} + w_3^* \cdot H_3^{12} + \dots + w_{12}^* \cdot H_{12}^{12}.$$

Відповідь: $w_{13,p} = -1,0641$.

Завдання 5. Обчислити короткостроковий прогноз:

$$\{y_{13,p}, y_{14,p}, y_{15,p}\}$$

значення змінної прогнозування Y на наступні 3 місяці за формулами:

$$y_{13,p} = y_{12}^* + w_{13,p},$$

де y_{12}^* – останнє значення згладженого часового ряду y_1, y_2, \dots, y_T .

$$y_{14,p} = y_{13,p} + w_{13,p},$$

$$y_{15,p} = y_{14,p} + w_{13,p}$$

Відповідь: $y_{13,p} = 24,269, y_{14,p} = 23,205, y_{15,p} = 22,14.$

2. Обчислення інтервальних прогнозів.

Один з *практичних підходів* до побудови *інтервальних прогнозів* $[d_{\tau}^*, g_{\tau}^*]$, для кожного моменту часу $\tau \in \{n + 1, n + 2, \dots, n + S\}$ базується на такому припущенні:

- Всі випадкові величини $(y_{n+1,p}; y_n^*; w_{n+1,p})$, які присутні в наведених формулах, мають нормальний розподіл.

При цьому припускається також, що:

- Прогноз $w_{n+1,p}$ можливого приросту w_{n+1} в момент часу $n + 1$ має нормальний розподіл з параметрами $(m_w; \sigma_w^2)$ де:

$$m_w = w^*_2 \cdot H_2^n + w^*_3 \cdot H_3^n + \dots + w^*_n \cdot H_n^n;$$

$$\sigma_w^2 = (w^*_2 - m_w)^2 \cdot H_2^n + (w^*_3 - m_w)^2 \cdot H_3^n + \dots + (w^*_T - m_w)^2 \cdot H_n^n.$$

Нехай y_{n+i} , $i \in \{1, 2, \dots, S\}$, означає точне (а нам невідоме) значення змінної прогнозування Y в момент часу $n + i$.

➤ *Помилкою прогнозу* називається число (e_{n+i}) , що визначається рівністю:

$$e_{n+i} = y_{n+i} - y_{n+i,p}, i \in \{1, 2, \dots, S\}.$$

Наступне припущення полягає в тому, що:

- *Помилка прогнозу* e_{n+i} має нормальний розподіл з параметрами:

$$E(e_{n+i}) = 0;$$

$$D(e_{n+i}) = \Sigma_{n+i}^2 = (H_n^n + H_{n-1}^n + H_{n-2}^n + \dots + H_{n-i+1}^n)^2 \cdot \sigma_w^2.$$

Задача побудови інтервального прогнозу для змінної прогнозування Y в момент часу $(n + i)$ формулюється наступним чином.

- ✓ Задане близьке до 1 число β .
- ✓ Необхідно визначити числовий інтервал $[d_{n+i}; g_{n+i}]$ таким чином, щоб виконувалась рівність:

$$P\{d_{n+i} < y_{n+i} < g_{n+i}\} = \beta.$$

Припустимо, що випадкова величина $N(0, \Sigma_{n+i}^2)$ має нормальний розподіл з параметрами $(0, \Sigma_{n+i}^2)$.

Знайдемо коефіцієнт $Z_{n+i}(\beta)$ з умови:

$$P\{-Z_{n+i}(\beta) < N(0, \Sigma_{n+i}^2) < Z_{n+i}(\beta)\} = \beta.$$

Тоді приймаючи до уваги припущення:

$$e_{n+i} = (y_{n+i} - y_{n+i,p}) \Leftrightarrow N(0, \Sigma_{n+i}^2)$$

отримаємо:

$$P\{-Z_{n+i}(\beta) < y_{n+i} - y_{n+i,p} < Z_{n+i}(\beta)\} = \beta.$$

Або:

$$P\{y_{n+i,p} - Z_{n+i}(\beta) < y_{n+i} < y_{n+i,p} + Z_{n+i}(\beta)\} = \beta.$$

Таким чином:

$$d_{n+i} = y_{n+i,p} - Z_{n+i}(\beta); g_{n+i} = y_{n+i,p} + Z_{n+i}(\beta).$$

3. Оцінка точності з допомогою нормального розподілу.

Завдання 6. Використовуючи знайдений в завданні 5 *точковий* прогноз попиту $\{y_{13,p}, y_{14,p}, y_{15,p}\}$, побудувати *інтервальний прогноз*

$$\{[d_{\tau}^*, g_{\tau}^*], \tau = 13, 14, 15\}.$$

З цією метою:

1) Вибрати ймовірність β рівною: $\beta = 0,95$.

2) Обчислити два параметри ($m_w; \sigma_w^2$) за формулами:

$$m_w = w^*_2 \cdot H_2^{12} + w^*_3 \cdot H_3^{12} + \dots + w^*_{12} \cdot H_{12}^{12}.$$

$$\sigma_w^2 = (w^*_2 - m_w)^2 \cdot H_2^{12} + (w^*_3 - m_w)^2 \cdot H_3^{12} + \dots + (w^*_{12} - m_w)^2 \cdot H_{12}^{12}.$$

Відповідь: $m_w = -1,0641; \sigma_w^2 = 4,7$.

3) Для кожного моменту часу $\tau = n + 1, \dots, n + S$; ($n = 12; S = 3$) обчислити дисперсію:

$$D(e_{n+i}) = \Sigma_{n+i}^2 = (H_n^n + H_{n-1}^n + H_{n-2}^n + \dots + H_{n-i+1}^n)^2 \cdot \sigma_w^2.$$

помилки прогнозу $e_{\tau} = e_{n+i}, i = 1, 2, \dots, S$.

Відповідь: $\Sigma_{n+1}^2 = 0,3542; \Sigma_{n+2}^2 = 0,9866; \Sigma_{n+3}^2 = 1,6714$.

4) Застосовуючи статистичні функції аркушу «Excel», що стосуються загального нормального розподілу $N(m; \sigma^2)$ з довільними параметрами ($m; \sigma^2$) («НОРМ.РОЗП» та «НОРМ. ОБЕР»), визначити для кожного моменту часу $\tau = n + 1, \dots, n + S$ ($n = 12; S = 3$) коефіцієнти $Z_{n+i}(\beta)$ з умови:

$$P\{-Z_{n+i}(\beta) < N(0, \Sigma_{n+i}^2) < Z_{n+i}(\beta)\} = \beta.$$

Відповідь: $Z_{n+1}(\beta) = 1,1665; Z_{n+2}(\beta) = 1,9468; Z_{n+3}(\beta) = 2,5339$.

5) Обчислити для кожного моменту часу $\tau = n + 1, \dots, n + S$; ($n = 12; S = 3$) межі $[d^*_{n+i}; g^*_{n+i}]$, які визначають *інтервальний прогноз* змінної прогнозування на заданому рівні надійності β :

$$d^*_{n+i} = y_{n+i,p} - Z_{n+i}(\beta); g^*_{n+i} = y_{n+i,p} + Z_{n+i}(\beta).$$

Відповідь: $d^*_{n+1,p} = 23,1, d^*_{n+2,p} = 21,26, d^*_{n+3,p} = 19,6$.

$g^*_{n+1,p} = 25,44, g^*_{n+2,p} = 25,15, g^*_{n+3,p} = 24,67$.

4. Використання функції Лапласа.

Завдання 7. Побудувати *інтервальний прогноз* $[d_{\tau}^*, g_{\tau}^*]$ змінної прогнозування, що відповідає заданому значенню *рівня надійності* β , для кожного моменту часу $\tau = T + 1, \dots, T + S$; ($T = 12$; $S = 3$) застосовуючи функції «НОРМ.СТ.РОЗП» та «НОРМ.СТ.ОБЕР» аркушу «Excel», (аналог функції Лапласа $\Phi(x)$).

З цією метою:

1) Для вибраної ймовірності β знайти коефіцієнт z_{β} з умови:

$$P\{-z_{\beta} < N(0; 1) < z_{\beta}\} = \beta.$$

де $N(0; 1)$ – нормальний стандартний розподіл.

Відповідь: $z_{\beta} = 1,9599$.

2) Для моменту часу $T + 1$ межі інтервалу $[d_{T+1}^*, g_{T+1}^*]$ визначаються за формулами:

$$d_{T+1}^* = y_{T+1,p} - z_{\beta} \cdot H_T^T \cdot \sigma_w = y_{T+1,p} - r_{T+1} \cdot \sigma_w;$$

$$g_{T+1}^* = y_{T+1,p} + z_{\beta} \cdot H_T^T \cdot \sigma_w = y_{T+1,p} + r_{T+1} \cdot \sigma_w.$$

Відповідь: $r_{T+1} = 0,538$; $\sigma_w = 2,168$; $d_{T+1,p}^* = 23,1$, $g_{T+1,p}^* = 25,44$.

3) Для моменту часу $T + 2$ межі інтервалу $[d_{T+2}^*, g_{T+2}^*]$ визначаються за формулами:

$$d_{T+2}^* = y_{T+2,p} - z_{\beta} \cdot (H_T^T + H_{T-1}^T) \cdot \sigma_w = y_{T+2,p} - r_{T+2} \cdot \sigma_w;$$

$$g_{T+2}^* = y_{T+2,p} + z_{\beta} \cdot (H_T^T + H_{T-1}^T) \cdot \sigma_w = y_{T+2,p} + r_{T+2} \cdot \sigma_w;$$

Відповідь: $r_{T+2} = 0,89798$; $\sigma_w = 2,168$; $d_{T+2,p}^* = 21,26$, $g_{T+2,p}^* = 25,15$.

4) Для моменту часу $T + i$, $i = 1, 2, \dots, S$, межі інтервалу $[d_{T+i}^*, g_{T+i}^*]$ визначаються за формулами:

$$d_{T+i}^* = y_{T+i,p} - z_{\beta} \cdot (H_T^T + H_{T-1}^T + H_{T-2}^T + \dots + H_{T-i+1}^T) \cdot \sigma_w = y_{T+i,p} - r_{T+i} \cdot \sigma_w;$$

$$g_{T+i}^* = y_{T+i,p} + z_{\beta} \cdot (H_T^T + H_{T-1}^T + H_{T-2}^T + \dots + H_{T-i+1}^T) \cdot \sigma_w = y_{T+i,p} + r_{T+i} \cdot \sigma_w.$$

Відповідь: $r_{T+3} = 1,16879$; $\sigma_w = 2,168$; $d_{T+3,p}^* = 19,6$, $g_{T+3,p}^* = 24,67$.

5. Графічна ілюстрація результатів.

Завдання 8. Побудувати в аркуші «Excel» графік точок

$$\{(1, y_1), (2, y_2), \dots, (n, y_n)\},$$

що представляють *емпіричні дані моделі* $\{y_1, y_2, \dots, y_n\}$.

Послідовно додати до нього графіки наступних точок:

- Графік точок

$$\{(1, y_1^*), (2, y_2^*), \dots, (n, y_n^*)\},$$

що представляє «згладжену» за допомогою *повзучого тренду* тенденцію розвитку часового ряду y_1, y_2, \dots, y_n .

- Графік точок

$$\{(\tau, y_{\tau,p}), \tau = n + 1, n + 2, \dots, n + S\},$$

точкового прогнозу

$$\{y_{n+1,p}, y_{n+2,p}, \dots, y_{n+S,p}\}$$

на момент часу $\tau = n + 1, n + 2, \dots, n + S$.

- Графік точок

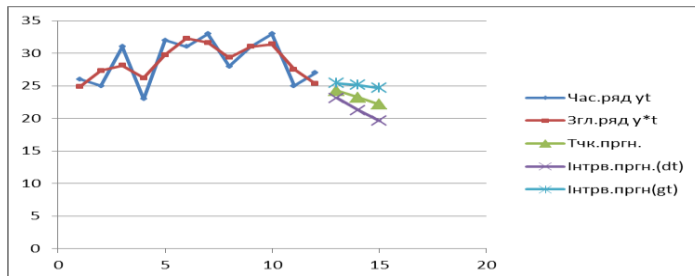
$$\{(\tau, d^*_{\tau}), \tau = n + 1, n + 2, \dots, n + S\},$$

що визначають *нижню межу інтервального прогнозу*.

- Графік точок

$$\{(\tau, g^*_{\tau}), \tau = n + 1, n + 2, \dots, n + S\},$$

що визначають *верхню межу інтервального прогнозу*.



4.17. Деякі особливості функціонування мережі Біткойн.

1. Емісія криптовалюти біткойн – «халвінг».
2. Вплив халвінгу на швидкість емісії біткойну.
3. Консенсус в мережі біткойна.
4. Вразливість мережі на «атаку 51%».

В підрозділі 3.15 підкреслювалось, що *майнінг* – це головний спосіб емісії нових крипто-монет. Нагадаємо, що цей термін пов'язаний з добуванням *корисних копалин*:

- Походить він від англ. «*mining*» і дослівно перекладається як «*видобуток корисних копалин*».

В мережі Біткойн цей термін означає процедуру емісії («*добування*») «*криптовалюти*»:

- Майнінг – це *протокол (алгоритм) розподіленого та децентралізованого консенсусу*.
- Полягає він в *дешифруванні даних і відбувається шляхом математичних обчислень*.

Кожен учасник мережі може взяти участь в цьому «*змаганні*», але переможець буде *тільки один* – саме він отримає всю нагороду:

- *Премію* за створення блоку та комісійні із всіх транзакцій, що включені до нього.

Творцеві мережі *блокчейн біткойн* Сатоші Накамото вдалося успішно розв'язати одну з головних проблем функціонування подібних платіжних мереж – загрозу *інфляції* в процесі зростання обчислювальних потужностей мережі.

Розглянемо, яким чином це відбувається.

1. Емісія криптовалюти біткойн – «халвінг».

В централізованих фінансових системах *інфляція* – це безпосередній наслідок *надмірної, нічим не обґрунтованої емісії* грошової маси (*фіатних*) грошей, що не забезпечені ніяким товарним еквівалентом.

Створюючи мережу *Біткойн* Сатоші Накамото заздалегідь попідкувався про те, щоб уникнути цього негативного явища

- Головним запобіжником *інфляції* є чітко визначена *верхня межа* для об'єму *«крипто-готівки»*.
- Кількість монет *«Біткойн»* в системі *не може перевищити* 21 млн. штук.

Емісія монет – це головний засіб мотивації учасників мережі до участі в процесі майнінгу.

- Тому наступним елементом, що передбачений для регулювання швидкості емісії біткойна та запобігання *інфляції* його вартості, є *халвінг*.
- Дослівно з англійської *«halving»* – це *«поділ навпіл»*, тобто зменшення в два рази розміру нагороди майнерам за додавання ними нового блоку в *блокчейн*.

Початкова винагорода становила 50 монет за створення блоку. Процедура *халвінгу* була програмно закладена в мережі біткойна її творцем Сатоші Накамото:

- Процедура *халвінгу* повинна була відбуватися через *кожні* 210 тисяч блоків, аж до моменту закінчення емісії криптовалюти, коли будуть отримані всі 21 млн запланованих монет.

За розрахунками *халвінг* має відбуватись приблизно раз на 4 роки, а емісія імовірно повинна припинитися в 2140 році, при цьому вже до 2036 р. буде отримано більше 99% всіх монет.

На даний момент відбулося вже чотири *халвінга*, а початкова майнінгова винагорода вже скоротилася в 4 рази:

- Перший *халвінг* відбувся 28 листопада 2012 року. Ціна біткойна в цей день становила 12\$. Від того моменту встановлена початкова винагорода була зменшена вдвічі і майнер за підтвердження блоку транзакції отримував 25 нових біткойнів.

- Другий *халвінг* відбувся 9 липня 2016 року. Ціна біткойна істотно збільшилась і становила 660\$.

Винагорода за новий блок була зменшена до 12,5 біткойнів.

- 11 травня 2020 року в мережі біткоіна на блоку #630000 відбувся третій в історії халвінг.

Вказаний блок, нагорода за який становила 6,25 BTC, в 19:23 GMT (або в 21:23 за київським часом) отримав пул AntPool. При цьому ціна одного біткойна дорівнювала вже приблизно 8600\$.

- Перед четвертим халвінгом, який відбувся 20 квітня 2024, ціна біткойна різко зросла і в день халвінга становила 64 262\$.

Винагорода за новий блок зменшилась і на даний момент становить 3,125 біткойнів.

Як підкреслювалось в [підрозділі 3.15](#), в грудні 2024 р. ціна біткойна досягнула позначки в 100 000\$ і продовжує зростати..

2. Вплив халвінгу на швидкість емісії біткойну.

В період між халвінгом біткоіна в 2016 та 2020 роками криптовалютна індустрія зростала по експоненті.

- Торгівельні об'єми BTC збільшились на 5000%, а їх ринкова вартість зросла на 1500%.
- Якщо в січні 2016 року показник середньомісячних торгових об'ємів біткоіна складав \$0,5 млрд, то в квітні 2020 перевищив \$27 млрд., тобто зріс майже в 50 разів.
- Якщо перед попереднім халвінгом ціна біткоіна знаходилась на рівні \$400, після чого зросла до кінця року вище \$800, а за весь проміжок – зросла в 15 разів.

В період зближення моменту третього халвінгу дехто з експертів та аналітиків ринку криптовалют передбачав, що багато майнерів відключать своє обладнання. Адже при винагороді 6,25 BTC за новий блок, обчислювальна потужність (*хеішрейт*) багатьох приладів, що добувають криптовалюту, зробить їх нерентабельними.

Ці прогнози відображались в статистиці фінансових ринків:

- Ціна біткоіна, піднявшись вище \$10 000 в кінці квітня 2020 р., по мірі наближення халвінга знижалась.

Падіння продовжувалось практично до самого моменту халвінга:

- За декілька годин до самої події, і на її момент перша криптовалюта торгувалася в районі \$8550.

Але ці побоювання не справдились.

➤ Вже в 20:02 GMT (або в 22:02 за київським часом), тобто 39 хвилин після моменту халвінга, Slush Pool знайшов блок #630001.

➤ Наступний #630002 блок з'явився через 28 хвилин.

➤ А вже блок #630003 відділяла від блоку #630002 лише одна хвилина.

Через 12 годин після халвінгу в мережі біткоїна спостерігався ріст транзакційних комісій, а всупереч очікуванням блоки добувалися навіть швидше, ніж до нього:

- Середній час знаходження трьох блоків складав менше 7 хвилин.

За 12 годин було добуто 79 блоків – що на 10% більше очікуваного показника, або на 5% більше очікуваних 144 блоків за добу.

Скоріше за все не так багато майнерів вимкнули своє обладнання. Не дивлячись на зниження величини нагороди, хешрейт біткоїна тримався в цілому на попередніх рівнях.

Наступні чотири роки, в періоді між третім (в 2020 р.) та четвертим (в 2024 р.) халвінгамим, ця тенденція збереглася та продовжує зміцнюватись.

3. Консенсус в мережі біткоїна.

Правила організації емісії *біткоїна* визначаються тільки комп'ютерним кодом його вільного програмного забезпечення.

Використовуючи спеціальне обладнання деякі користувачі (*вузли*) мережі, яких називають *майнерами*, верифікують (*перевіряють*), зберігають та гарантують безпеку транзакцій в *блокчейні*.

Теоретично майнером може бути кожен:

- ✓ Вистачить запустити «*Bitcoin Core*» (проект з відкритим вихідним кодом, що підтримує та випускає програмне забезпечення клієнтів біткоїну) та перевірити правильність всіх проведених операцій.

Ця особливість протоколу, що забезпечує *відкритість* та *прозорість біткоїну*, є його безсумнівною перевагою:

- ✓ Кожен має можливість пересвідчитись, що все йде вірним шляхом.

Істотна перевага *блокчейн* мереж в порівнянні з «*традиційними*» фінансовими системами полягає в серйозному їх захисті від *несанкціонованого* втручання, гарантованому надійними *криптостійкими математичними алгоритмами*. Для того, щоб затвердити та зареєструвати в мережі будь-яку операцію, вона повинна бути *перевірена*.

На *вході* транзакція отримує посилання на попередню транзакцію, яка підтверджує той факт, що згадані в умові кошти – реальні.

На *виході* вона генерує один, або декілька *біткоїн-адрес* з відповідними приписаними до них сумами:

- ✓ Кошти на вході та виході будь-якої транзакції завжди *збалансовані*.

Ця нова транзакція не відразу визначається як допустима – її необхідно ще включити до реєстру угод (*блоків*). Щоб стати законною кожна транзакція повинна бути *підписана (зашифрована)* за допомогою асиметричного шифрування.

- ✓ Транзакції, передані в незакодованому вигляді, признаються дійсними за допомогою відповідних *закодованих підписів*, що візують умову.

Кількість подібних щоденних умов стрімко зростає (дані за 2016 р.: в червні – 200 000, в листопаді – 300 000). Третій халвінг на блоку #630000 відбувся 11 травня 2020 р. Четвертий, на блоку #840 000 – 20 квітня 2024 р.

Однією із суттєвих *вад* блокчейн біткойна в порівнянні з традиційними технологіями проведення транзакцій є *відносна повільність*:

- ✓ Якщо потужність платежів мережі «*Visa*» складає 56 000 транзакцій в секунду, то в мережа *біткойна* побудована таким чином, що опрацьовує в середньому біля 7 (семи!) транзакцій в секунду.

При укладенні кожної умови тисячі майнерів запускають обчислення спрямовані на її перевірку та включення до реєстру угод. Але тільки один знаходить рішення, з яким повинні погодитись всі інші.

- Їх мотивує сподівання *отримати нагороду* за цю працю, що підтримує безпеку мережі.

Блокчейн зберігає *слід* кожної умови, але в ньому немає *загального балансу* кожного окремого користувача (на відміну від банку, де клієнт може мати кілька рахунків з усіма відомостями, що стосуються кожного з них).

Користувач блокчейну має в себе на власних носіях «*гаманець*» в якому зберігається *закритий ключ*, натомість *відкритий ключ* записується в блокчейні і є *недоторканим* (так працює система асиметричного шифрування «*закритий ключ / відкритий ключ*»).

- Втрата *закритого ключа* призводить до втрати пов'язаних з ним біткойнів.

Ми вже звертали увагу на можливість виникнення конфлікту, коли одночасно будуть запропоновані різні рішення:

- Частина вузлів визнає одне з них,
- Інша частина – інше.
- Це призведе до появи розгалуження в ланцюгу блоків.

Принцип *колективного консенсусу*, реалізований в мережі Біткойн, керується наступним правилом:

- Якщо утворюється розгалуження в ланцюгу блоків, то мережа приймає за істинне *довше серед них*.

Таким чином:

- *Коротше* відгалуження ігнорується мережею і відкидається з усіма блоками (а значить і транзакціями, розміщеними в них), що до цього відгалуження потрапили.

4. Вразливість мережі на «атаку 51%»..

Незважаючи на те, що *блокчейн* мережа (на відміну від «традиційних» фінансових систем) захищена від *несанкціонованого* втручання надійним *криптостійким математичним забезпеченням*, вона, на жаль, теж має свої «вразливі» ситуації, які навіть теоретично не можна подолати.

З іншого боку, щоправда, *шанси* практичної реалізації подібних ситуацій в нинішніх умовах майже *нульові*. Йдеться, зокрема, про загрозу «атаки 51%».

➤ Подібна загроза виникає тоді, коли в мережі з'являється вузол (або їх об'єднана група), що *контролює понад 50%* обчислювальних потужностей.

Тоді домінування цієї групи, що об'єднана спільною метою, може дати їй можливість контролювати всю мережу.

- Маючи можливість створювати нові блоки швидше за інших, вони зможуть повністю забирати всю винагороду за *майнінг* та нові транзакції.
 - Зможуть також на свій розсуд реалізовувати операції, залишаючи поза увагою ті, що їх не цікавлять.
- Але найбільша загроза – це *повторне використання* тих самих монет, тобто так звані «*подвійні витрати*».

Пояснимо коротко, як це можливо. Можливість появи відгалужень та ігнорування мережею розміщених в них транзакцій означає, що сам факт включення операції до якогось блоку ще не свідчить про їх реалізацію.

- Потрібний певний час, щоб переконатися, що транзакція відбулась, а не потрапила до такого відгалуження.
- В мережі Біткойн вважається, що будь-яке відгалуження не може бути *довше*, ніж *6 блоків*.

Ймовірність такої події *практично нульова*, а значить *шести підтверджень* (один блок – одне підтвердження) цілком достатньо, щоб вважати транзакцію *реалізованою*.

- На практиці – це приблизно *година* часу.

Припустимо тепер, що існує «*зловмисник*», який контролює понад 50% обчислювальних потужностей мережі, та покажемо, як він зможе використати цю обставину для реалізації «*подвійної витрати*».

Він обирає в якості «*пункту відліку*» певний конкретний блок, та починає проводити паралельно два процеси:

- ✓ Створювати нові блоки та формувати з них відгалуження, не демонструючи до певного моменту його мережі.

В цих блоках зловмисник *не буде* використовувати свої активи.

- ✓ Одночасно з цим він буде проводити операції в основній мережі, витрачаючи свої кошти, та чекати їх підтвердження мережею.

Тобто буде чекати того моменту, коли після блоку з його транзакціями з'явиться ще 5 нових блоків.

Після цього він розкриє для всієї мережі створений ним паралельно ланцюг блоків, в якому починаючи з «пункту відліку» буде зовсім інше відгалуження.

- Маючи обчислювальну перевагу над рештою мережі йому вдасться *створити довший ланцюг валідних блоків*, ніж це було в основній мережі.

Отже мережа буде вимушена визнати його відгалуження *істинним*, а всі «старі» блоки (починаючи з «пункту відліку») раніше розраховані та підтверджені мережею, відкинути.

- Такі блоки отримують статус «*orphanedblocks*», тобто «*осиротілих*», таких, що втратили зв'язок з мережею.

Разом з цим будуть відкинуті всі видаткові транзакції «*зловмисника*», ніби їх не було взагалі.

- Він повертає витрачені вже один раз кошти і мережа вимушена з цим погодитись.

Варто зауважити, що в історії мережі Біткойн був випадок, коли природнім шляхом створилася ситуація можливої «*атаки 51%*»:

- 13 червня 2014 р. на протязі кількох годин пул *Ghash* отримав контроль над 51% обчислювальних потужностей мережі.

Реакція самих учасників пулу була миттєвою:

- Багато хто з них *припинили майнінг*;
- А сам пул *припинив реєстрацію* нових користувачів.

- Втрата довіри до криптовалюти – це *найстрашніший* наслідок можливого контролю над мережею та «*атаки 51%*».
- Це неминуче призведе до падіння її вартості, вираженої в «*класичному*» *фіатному* еквіваленті.

В цьому на сьогоднішній день *основна цінність* цифрових грошей, і це в першу чергу стосується найактивніших її *майнерів*.

- Обмін заробленої *криптовалюти* на валюту *фіатну* – це для них повсякденна необхідність.

Слід відзначити, що загальна обчислювальна потужність мережі в даний момент настільки «*астрономічно-велика*», що повторення ситуації з червня 2014 р. *неможливе*.

4.18. «Ethereum», криптовалюта «ефір» та «смарт-контракти».

1. Блокчейн індустрія, «криптовалютне золото». 2. Проект «Ethereum» та «криптовалютне срібло». 3. «Система скриптів» в мережі «Біткоїн». 4. Формування адреси та блоків в мережі «Ethereum». 5. Криптоактиви в мережі «Ethereum»: «ефір» та «газ». 6. Майнінг в мережах «Біткоїн». та «Ethereum». 8. Принципи «Proof-of-Work» та «Proof-of-Stake».

1. Блокчейн індустрія, «криптовалютне золото».

Проект цифрових монет *біткоїн*, створений понад 16 років тому, став дуже успішним *піонером-першопрохідцем* в найновітнішій високотехнологічній галузі, яка повстала на основі технології *Блокчейн*.

➤ 16 років в ІТ галузі – це *величезний* проміжок часу, можна сказати – ціла *епоха*.

Фактично від моменту появи системи *Блокчейн Біткоїн* розпочалися спроби створення більш досконалих, прогресивніших криптовалютних проектів.

В певний момент цей процес прийняв лавиноподібний характер і нині функціонує понад *дві тисячі* крипто валют, які отримали принаймні одну біржову оцінку на фінансовому ринку. І хоч багато представників потужної криптоіндустрії вважає (і небезпідставно) проект *Біткоїн* *застарілим* та *невідповідним* до сучасних вимог, його авторитет в цій сфері *абсолютний* і *безсумнівний*.

➤ Сумарна капіталізація на фінансовому ринку всіх інших разом взятих криптовалют *порівняльна* з капіталізацією біткоіна.

Не випадково всі вони мають ще одну спільну назву – «*альткоїн*», тобто «*альтернатива біткоіна*». Переважна їх більшість – це «*біткоїноподібні*» клони, що взагалі не відрізняються, а якщо і відрізняються, то в дрібних деталях, від *Блокчейн Біткоїн*.

Зрештою сам проект *Біткоїн* був не чим іншим, як звичайною *децентралізованою платіжною системою* (підкреслимо – досить «*примітивної*» за своїми можливостями).

- Його революційність полягала у використанні технології *Блокчейн*, а сам проект започаткував нову індустрію, що базувалася на цій технології.
- Аналіз досвіду функціонування цього проекту дозволив фахівцям оцінити всі можливості та переваги технології *Блокчейн*.

В свою чергу, індустрія, що бурхливо розвивалася, формувала запити на більш складний функціонал *блокчейн-систем*. З'явилася необхідність створення нових *технологічних* засобів, які б дозволили будувати *децентралізовані* мережі найрізноманітнішого призначення, в тому числі і платіжні, на новому якісному рівні.

2. Проект «Ethereum» та «криптовалютне срібло».

Першим вдалим кроком в цьому напрямку і успішною спробою *якісної* зміни проекту *Bitcoin* в багатьох його технологічних аспектах, був проект «Ethereum».

В кінці 2013 р. редактор журналу «*Bitcoin Magazine*» канадський програміст російського походження Віталік Бутерін опублікував в ньому опис цього проекту.

➤ Невдовзі, 30 липня 2015 р. платформа «Ethereum» була успішно запущена.

Нині загальна її капіталізація становила понад \$30 млрд. щоденно в мережі «Ethereum» здійснюється більше ніж півмільйона транзакцій, а по своїй популярності та по всім іншим параметрам криптовалюти вона фактично від самого початку свого існування надійно утримує *друге місце* після *Bitcoinу*.

«Ефір» обертається практично на всіх біржах, що пропонують послуги в сфері торгівлі *криптовалютою*. І якщо *Bitcoin* називають в фінансових колах «*криптовалютне золото*», то *Ефір* отримав серед учасників криптовалютиного ринку почесний «*титул*» «*криптовалютного срібла*».

Платформа «Ethereum» проектувалась вже не як виключно платіжна мережа:

➤ Це була *Блокчейн-система* нового покоління, на базі якої, зокрема, може бути реалізована децентралізована платіжна системи, подібна *Блокчейн Bitcoin*.

Найголовніше нововведення, яке вдалося успішно втілити Віталіку Бутеріну в проекті «Ethereum», пов'язане з можливістю реалізації більш складних в порівнянні з простим переказом цифрової готівки операцій:

➤ Так званих «*розумних*» (або «*смарт*») контрактів.

Автором концепції «*смарт-контрактів*» є Нік Сабо, який ще в 1994 р., задовго до появи перших *Блокчейн-систем*, запропонував форму контрактів, які можна реалізувати в розподіленій децентралізованій електронній мережі. Сабо визначив цей тип угод наступним чином

- Протокол *передачі інформації*, яка забезпечує автоматичне виконання сторонами умов угоди.

На відміну від «*звичайних*» контрактів, в яких часто умови викладені *нечітко*, мають *описовий* характер, та можуть по-різному тлумачитись:

➤ «*Смарт-контракт*» контролює лише ті умови, які можна *чітко математично* довести.

3. «Система скриптів» в мережі «Біткоїн».

Ідеям Ніка Сабо судилося бути вперше втіленими (в повному їх вимірі) в ділову практику лише через понад 20 років після їх проголошення, в проекті «Ethereum» Віталіка Бутеріна.

Варто відзначити, що деякі «прояви» технології «Смарт-контрактів» спостерігаємо вже в проекті Блокчейн Біткоїну.

Головною функцією Блокчейн Біткоїну було переведення крипто-активів з одної адреси на іншу. Транзакція, як правило, формується наступним чином. Відправник, формуючи свою операцію, вказує в незакодованому вигляді:

- *На вході* – посилання на транзакцію, що підтверджує реальність коштів умови;
 - *На виході* – одну або декілька «Біткойн» – адрес з відповідними (збалансованими) приписаними до них сумами.
- Для того, щоб отримати статус «достовірної» або «законної», незакодована угода повинна бути підписана (завізована) електронним підписом, сформованим за допомогою методів асиметричної криптографії.
- Для того, щоб отримати статус «допустимої» і потрапити до реєстру транзакцій, операція повинна *пройти успішно перевірку* всіх учасників мережі.

Далі реалізацією угоди займаються *майнери* і вона повинна потрапити до нового блоку, який буде *прийнятий* системою.

- Сформувавши блок *майнер* автоматично активує програмні засоби, що здійснюють в мережі передбачені в транзакції перекази.

Оскільки зміст всіх операцій практично однаковий, то головний критерій формування нового блоку визначався встановленим а мережі «Біткойн» обмеженням:

- Розмір блоку не перевищує *один мегабайт*.

Враховуючи більш-менш стандартний вигляд операції її розмір (в сенсі програмної реалізації) теж *більш-менш стандартний*:

- В середньому біля 300 байт.

Звідси всі інші параметри, що характеризують функціонування Блокчейн Біткоїну.

Однак Сатоші Накамото вже ввів деякі елементи «смарт-контрактів» до своєї мережі. Так серед параметрів *виходу* переважної більшості транзакцій Блокчейну Біткоїн присутня команда:

- “P2PKH”, тобто “Pay to Public Key Hash”.

Ця команда, власне, і *реалізує* процедуру оплати на *хеш* публічного ключа, яким і є біткоїн-адреса отримувача транзакції.

Створюючи платіжну систему Накамото передбачав, що навіть найпростіші операції можуть мати певні особливості:

➤ Тому він оснастив систему спеціальною спрощеною мовою програмування – так званою «системою скриптів».

Ця мова містила біля 80 команд, кожна з яких виконувала певну алгоритмічну процедуру.

Тому крім стандартної форми платежу «P2PKH» можна було реалізувати кілька нестандартних. Наприклад:

- Використати мульті-підпис,
- Використати кошти раніше вказаного терміну, тощо.

Хоча цей вибір був дуже обмежений.

4. Формування адреси та блоків в мережі «Ethereum».

Зупинимось коротко на тих *нових елементах*, які вніс проект «Ethereum» в практику створення криптовалютних *блокчейн-систем*.

✓ Адреса користувача – це його «*обличчя*», або «*візитка*» в мережі, підтвердження його присутності та суб'єктності в системі.

Алгоритм створення адреси в мережі «Ethereum» схожий до того, що використовується в мережі *блокчейн біткоїн*.

- Головна відмінність полягає в тому, що відсутній заключний крок алгоритму «Біткоїн»: *Хеш відкритого ключа не перетворюється* в більш «зручний» для використання вигляд, а залишається практично без змін.
- ✓ Пояснюється це тим, що «Ethereum» не створювалась, як виключно *платіжна система*, в якій споживачу необхідно постійно *вручну* вводити адреси при формуванні транзакцій.

Суттєво відрізняється принцип формування блоків в мережі «Ethereum».

✓ Проект «Ethereum» створювався, як децентралізована розподілена система для реалізації «*розумних контрактів*».

Іншими словами:

- «Ethereum» це система для реалізації найрізноманітніших угод, що виконуються *без втручання «третіх сторін»*.

Тому, на відміну від «*скриптів*» «Біткоїна», код «*смайт-контракта*» пишеться в мові програмування, що задовольняє всім вимогам повноти.

- Найпопулярнішою в «*Etherium*» є *об'єктно-орієнтована* мова програмування «*Solidity*».

Мова «*Solidity*» семантично подібна до популярної мови програмування «*JavaScript*».

В цілому процес формування «*смайт-контракту*» в системі «*Etherium*» схожий на звичайну транзакцію, яка, однак, має ряд додаткових елементів.

Це, перш за все:

- Програмний код, про який йдеться.

Кожен учасник мережі має можливість створювати «*смайт-контракти*».

- Для цього він мусить описати алгоритмічну логіку обробки угод у вигляді програмного коду та помістити його в *блокчейн*.

✓ З цього моменту «*смайт-контракт*» *присутній* в системі.

Будь-хто з бажаючих учасників мережі може активізувати його роботу, відправляючи транзакції *на адресу контракту* в мережі.

Іншими словами:

- Контракт перетворюється в повноправний суб'єкт мережі, що може *приймати* та *формувати* транзакції.

Але робить він це не самостійно:

✓ Для цього в системі «*Etherium*» існує так звана «*віртуальна машина Ethertum*», покликана реалізувати програмний код *смайт-контракту* децентралізованим чином.

- При створенні нового блоку з її допомогою *майнер* і запускає на виконання програмний код контракту.
- Крім цього *смайт-контракт* може запустити не тільки майнер, а й *будь-який інший вузол мережі*, наприклад коли перевіряє на валідність отримані від майнера блоки.

З точки зору програмного втілення і, як наслідок, об'єму необхідних обчислень, в процесі реалізації програмного коду, далеко не всі передбачені в системі «*Etherium*» контракти є рівнозначними між собою.

- Для втілення одних достатньо кілька рядків;
- В той час, як інші – це складні алгоритми, що потребують тисячі таких рядків

Очевидно, що їх обробка також вимагає різної кількості процесорного часу. Це принципово змінило підхід до вибору *критеріїв* формування блоків в системі «*Etherium*».

- ✓ Розмір блоку обмежується не кількістю *байтів* (як це було в мережі «*Біткойн*»), а *обчислювальною потужністю*, необхідною на обробку даних блоку.

Тому розмір блоку мережі «*Etherium*» визначає:

- *Сукупний об'єм обчислень*, потрібний на його обробку.
- ✓ В середньому один блок складають *приблизно 400* стандартних транзакцій.

5. Криптоактиви в мережі «*Etherium*»: «ефір» та «газ»..

Кількісною мірою сумарних обчислень, пов'язаних з реалізацією конкретного контракту в мережі «*Etherium*», служить необхідний для цього об'єм «газу».

- ✓ «Газ» – це немонетарна, а виключно «*кількісна*» величина:
 - В систему закладені чіткі та конкретні «*цінники*», що дозволяють точно розрахувати яка кількість газу буде витрачена на реалізацію *смарт-контракту*.

Для кожного оператора байт-коду мережі «*Etherium*» існує його фіксована «*вартість*», виражена в одиницях газу.

Фактично в системі «*Etherium*», існує два види *криптоактивів*, тобто два види цифрових платіжних засобів.

- ✓ *Основною криптовалютою* системи «*Etherium*» є цифрові монети «ефір».

Ця криптовалюта використовується як для розрахунків *всередині* мережі, (для оплати *комісійних* та винагород за *майнінг*, тощо), так і на *зовнішніх* ринках (*криптовалюта*, що продається на біржах).

На відміну від біткойна, який поділено на 100 млн. частин (мінімальне значення в 8-му знаку після коми), «ефір» поділено на *квінтіліон* частин (мінімальне значення в 18-му знаку після коми).

- Найдрібніша частинка дістала назву «*Wei*», на честь творця проекту «*B-money*» Вей Дая.
- Одна мільйонна частинка *ефіру* названа «*Szabo*» в честь винахідника *смарт-контракт* та творця системи «*Bit Gold*» Ніка Сабо.
- Одна тисячна частинка *ефіру* отримала назву «*Finey*» на честь Хела Фінні, контрагента Сатоші Накамото в самій першій операції в мережі «*Біткойн*» в січні 2009 р.

Ще одна суттєва відмінність *ефіру* від біткойна:

- Емісія монет *ефіру* жодним чином не обмежена.

Загальна їх кількість давно перевищила 100 млн.

- ✓ Другим платіжним засобом системи «*Etherium*» є цифрові монети що мають назву «*газ*».

Крім основної криптовалюти – *ефіру*, в системі «*Etherium*» передбачена оплата обчислювальних потужностей при обробці смарт-контрактів за допомогою спеціально створеного платіжного засобу, що має назву «*газ*».

- Це своєрідне «*паливо*», необхідне, щоб реалізувати програмний код смарт-контракту.

Створюючи мережу «*Etherium*» Віталік Бутерін планував використовувати перш за все «*ефір*» для сплати вартості «*газу*» при обробці контрактів.

- Спрямовуючи в мережу транзакцію її відправник приблизно (але з запасом) вказує, яку *максимальну* кількість «*газу*» він готовий «*спалити*», щоб реалізувати контракт.
 - Точне значення встановить *майнер* при формуванні блоку, а різницю (*переплату*, якщо така буде) поверне.
- ✓ Ціноутворення на «*газ*», виражене в «*основній*» криптовалюті, визначається *навантаженням* на мережу.

6. Майнінг в мережах «*Біткоїн*». та «*Etherium*».

Перш за все при проектуванні системи було прийнято рішення, що блоки будуть формуватися *швидше*, ніж в *Блокчейн Біткоїн*.

- ✓ Середній час створення блоку – 30 секунд.

Це в 50 разів швидше, ніж в мережі *Біткоїн*, тому не дивлячись на те, що «*Etherium*» запущений значно пізніше ніж «*Біткоїн*», нині в «*Etherium*» блоків більше, ніж в «*Біткоїн*».

Не дивлячись на те, що Віталік Бутерін використав для знаходження нових блоків той самий принцип «*доведення роботи*» («*Proof-of-Work*»), що й Сатоші Накамото, реалізований він в «*Etherium*» зовсім інакше.

- ✓ Зрозуміло, що для прискорення процесу знаходження валідних розв'язків, значно знижено *ступінь складності* обчислювальної задачі.

Але головною відмінністю мережі «*Etherium*» є те, що *сумтєво відрізняється зміст задачі*.

В мережі «*Біткоїн*» процедура майнінга фактично зводиться до пошуку підходящого значення «*нонса*», яке необхідно додати до заголовку блоку, щоб отримати «*золотий хеш*» з необхідною кількості *нулів* на початку. Тому розв'язок передбачав *простий перебір* та перевірку астрономічної кількості можливих варіантів.

➤ Як правило, застосовувався алгоритм SHA-256, з використанням для його реалізації пристроїв ASIC.

Теоретично кожний учасник мережі може бути майнером. Знаряддям праці майнера є спеціальний пристрій, який теж називають «майнером». Найбільш продуктивні пристрої для майнінгу – це «асіки», або «інтегральні схеми для специфічного застосування».

Слово «асік», походить від англійської аббревіатури:

- ASIC – *Application-specific integrated circuit*.

Тобто інтегральна схема спеціалізована для вирішення конкретного завдання. Оскільки вона застосовується в конкретному пристрої і виконує строго обмежені функції, то на відміну від інтегральних схем загального призначення значно швидша і дешевша, а отже – ефективніша.

➤ Наступне коло проблем пов'язане з *обчислювальною потужністю* обладнання на якому виконується майнінг.

При цьому поняття «*потужність*» вживається в значенні *швидкості виконання математичних операцій*, отже враховуються як технічні характеристики та параметри апаратури, на якій виконуються обчислення (тобто пристрої ASIC, або *відео карта* та процесор комп'ютера «*ферми*»), так і ефективність алгоритмі, що лежать в основі цих розрахунків. Адже праця, а головне – її наслідки майнерів базуються на принципі:

- Або все, або нічого.

Майнери обробляють транзакції, що підтримує та гарантує безпеку мережі, а за це в якості нагороди отримують нові *біткоіни*. При кожній угоді тисячі майнерів, тобто окремих користувачів (*вузлів*) мережі отримують такий самий масив *необроблених даних* та запускають обчислення. Коротко мету цих обчислень можна охарактеризувати наступним чином:

- Підбір вірного значення с врахуванням заданих правил.

Той хто першим знайде розв'язок і буде переможцем, він і отримає винагороду. При цьому знайдений розв'язок надасть угоді статус «*дійсної*». Варто підкреслити, що кожного разу учасників тисячі, а переможець тільки один, тому існує ризик «*працювати вхолосту*», тобто:

- Участь в процесі обчислень ваше обладнання *буде приймати*, але нагороди ви *не отримаєте*.

Саме для вимірювання такої «*узагальненої*» обчислювальної потужності систем *майнінгу* крипто валют (тобто пристроїв, що добувають криптовалюту) використовується параметр під назвою *хеширейт*. На практиці обчислювальна потужність таких пристроїв виражається в (*хеши/сек*), тобто кількістю *хешей*, що розраховуються за секунду.

- Кілохеш кН – 1000 h/s; Мегахеш МН – 1 млн h/s; Гігахеш ГН – 1 млрд h/s; Терахеш НН – 1 000 000 000 000 (12 нулів) h/s; Петахеш – РН – 1 000 000 000 000 000 (15 нулів) h/s.

Перші пристрої ASIC, що були виготовлені в червні 2012 р. компанією «*Butterfly Labs*», працювали з *хеширештом* 4,5 Гігахеш за секунду. Це приблизно в 600 разів швидше, ніж це робив Сатоші Накамото. При мінімальній складності *валідний хеш* знаходиться протягом секунди.

Пристрої ASIC фірми «*Bitmain*» зразка 2019 р. виконують перебір хешей зі швидкістю 53 Терахеш за секунду, тобто більше ніж в 10000 разів швидше від перших подібних пристроїв 2012 р. А *хеширешт* всієї мережі на своїх пікових показниках досягав *космічних значень* – 60 *ексахешей* за секунду, тобто $6 \cdot 10^{19}$ хешей за секунду.

Про що це говорить?

- Нині ніхто, ані окремих індивідуум, ані конкретна окрема фірма, *самостійно* виконати *майнінг* хоча б одного блоку в мережі *Блокчейн Біткоїн* не може. (Хіба що випадковим чином!)

В мережі «*Etherium*» використовується зовсім інший алгоритм пошуку валідних розв'язків, якому розробники дали назву «*Ethash*». Реалізація цього алгоритму вимагає використання значно більшого об'єму оперативної пам'яті:

- В оперативній пам'яті розміщені додаткові дані, потрібні для коректної роботи алгоритму.

Дуже часте звернення до оперативної пам'яті призводить до того, що *майнер* для добування «*ефірів*», працює в *десятки тисяч* разів повільніше, ніж його *біткойновий* аналог. Це дає можливість значною мірою захиститися від появи *ASIC-пристроїв* для мережі «*Etherium*».

Такий підхід дозволив повернутися до майнінгу монет «*ефіру*» з допомогою графічних процесорів відеокарт звичайних комп'ютерів і суттєво підвищити ступінь *децентралізації* процесу створення нових блоків. Але головний наслідок цього рішення:

- ✓ Значна економія електроенергії:
 - Мережа «*Etherium*» споживає майже втричі менше електроенергії, ніж мережа «*Біткоїн*».

Однак це споживання все ще залишається дуже великим.

Варто також зауважити, що розробники системи «*Etherium*» планують найближчим часом докорінно переглянути принципи створення нових блоків ланцюга.

- ✓ Нині мережа «*Etherium*» знаходиться в процесі поступової відмови від *майнінгу* на основі протоколу «*Proof-of-Work*» («*доведення роботи*») на користь принципу «*Proof-of-Stake*» («*доведення володіння*»).

Рекомендовані літературні джерела:

1. Wojna A.: *Analiza statystyczna oraz prognozowanie w modelach ekonomicznych*. Część 1. *Wprowadzenie do statystyki opisowej, rachunku prawdopodobieństwa i statystyki matematycznej*. Koszalin, PK 2003.
2. Wojna A.: *Analiza statystyczna oraz prognozowanie w modelach ekonomicznych*. Część 2. *Metody oraz narzędzia prognozowania zjawisk ekonomicznych*. Koszalin, PK 2004.
3. Wojna A.: *Predykcja ekonometryczna oraz stochastyczne modelowanie* Część 1. Koszalin, PK 2007.
4. Wojna A.: *Ryzyko w procesach finansowych oraz metody badań koniunktury*. Koszalin, PK 2009.
5. Wojna A.: *Wykłady z podstaw statystyki*. Część 1. *Opis statystyczny*. Koszalin, PK 2011.
6. Wojna A.: *Wykłady z podstaw statystyki*. Część 2. *Elementy wnioskowania statystycznego oraz matematyczne metody pomiaru ryzyka*. Koszalin, PK 2015.
7. О.А. Война «Економічний ризик. Математичні моделі та методи керування». – Київ. ВПЦ «Київський університет», 2001, – 100 с
8. Box G.E.P., Jenkins G.M.: *Time Series Analysis: Forecasting and Control*. San Francisco: Holden-Day 1976.
9. Green W. H.: *Econometric analysis*. Macmillan, New York 1993.
10. Kotler P.: *Marketing Management*. Englewood Cliffs: Prentice-Hall 1988.
11. Welfe A.: *Ekonometria. Metody i ich zastosowanie*. Warszawa PWE 1995.
12. Опарін В. М. та ін.: «Фінанси». – К: Знання, 2006, – 247 с.
13. Imran Bashir. «*Mastering Blockchain*». – Birmingham - Mumbai. Packt Publishing. 2018, – 538p.
14. William Mougayar. «*The Business Blockchain*». – JohnWiley&Sons, Inc. 2016, – 216 h.
15. Laurent Leloup. «*Blockchain: La revolution de la confiance*». – 2017, Groupe Eyrolles, Paris, France – 256 p
16. Daniel Drescher. "Blockchain Basics: A Non-Technical Introduction in 25 Steps", – 2017.
17. Andreas M. Antonopoulos. "Mastering Bitcoin: Programming the Open Blockchain". – 2017.
18. A.O. Petters, X. Dong “An Introduction to Mathematical Finance with Applications” Springer Undergraduate Texts in Mathematics and Technology, 2016.
19. Marco Corazza, et. al. “Mathematical and Statistical Methods for Actuarial Sciences and Finance”, Springer International Publishing AG, Cham, 2018.
20. О.В. Виноградова, Н. С. Гончар: «Фінансова математика». – Київ. 2020.
21. В.Р. Кучеренко, В.А.Карпов: «Основи економічної кон'юнктури»: – Київ. Центр навчальної літератури, 2004..