

результати тестування роботи основних складових підсистеми, що підтверджує коректність та правильність роботи підсистеми.

Література

1. [Електрон. ресурс]. – Доступний з: http://sourceforge.net/softwaremap/trove_list.php?form_cat=621.
2. **Lukasiewicz, Jan** (1957). Aristotle's Syllogistic from the Standpoint of Modern Formal Logic: Oxford University Press.
3. **Курейчик В.В., Нужнов Е.В.** Возможности организации интегрированной инструментальной среды поддержки процедур генетического поиска и оптимизации решений // Новости искусственного интеллекта, 2003. – № 5. – 236 с.
4. **Michalewicz, Zbigniew**. Genetic algorithms + data structures = evolution programs. – 3rd rev. and extended ad, Springer – Verlag Berlin Heidelberg New York, 1996. – P. 141-149.

УДК 681.3+519.6

Доц. О.А. Пастух, канд. техн. наук –
Європейський університет, Тернопільська філія

МАТЕМАТИЧНИЙ ФОРМАЛІЗМ ФУНКЦІОНУВАННЯ КВАНТОВОГО ПРОЦЕСОРА

Розглянуто математичний формалізм функціонування квантового процесора, охоплює математичний опис станів квантових бітів регістра квантового процесора у вигляді комплексного векторного простору хвильових функцій. Наведено математичний опис квантової статистичної моделі, яка інтегрує у собі основні стадії (запис, обчислення, вивід) роботи квантового процесора і показано неспроможність використання класичної статистичної моделі для цих потреб. Математичний опис однокубітних, двокубітного та багатокубітних логічних елементів (унітарних операторів).

Assoc. prof. O.A. Pastukh – European university, Ternopol department

Mathematical formalism of functioning quantum processor

Mathematical formalism of functioning quantum processor has been analyzed. It include mathematical description of states of quantum bits of register of quantum processor as of complex vector space of wave functions. Mathematical description of quantum statistical model if integrate bases phases (enter, computation, output) of operation quantum processor and show impossibility of classical statistical model for needs. Mathematical description of logical gates for one quantum bit, two quantum bit and many quantum bits (unitary operators).

Вступ. Все більше науковців, які працюють у сфері інформаційних технологій, у своїх роботах проявляють інтерес до квантових інформаційних технологій, зокрема до їх основного обчислювального елемента – квантового процесора. Це зумовлено тим, що квантовий процесор має ефект квантового паралелізму та квантової інтерференції, які розширюють його обчислювальні можливості порівняно з класичним процесором. Основою роботи квантового процесора, крім фізичної реалізації, є математичне забезпечення – математичний формалізм його функціонування.

Аналіз досліджень і публікацій. Математичний апарат, який використовується для математичної формалізації функціонування квантового процесора використовує надбання квантової теорії, теорії алгоритмів та ін. і висвітлений у багатьох роботах, як іноземних [1, 2], так і українських [3, 4] вчених.

Постановка завдання. З великого об'єму надбань математичного апарату квантової теорії, теорії алгоритмів та ін. висвітлити основи математичного формалізму функціонування квантового процесора.

Основна частина. Квантовий процесор (q -процесор) – це пристрій, який виконує квантові логічні операції (унітарні перетворення), що не руйнують квантової суперпозиції протягом квантових обчислень. Схематично q -процесор можна зобразити, як показано на рис. 1, а його роботу представити у вигляді послідовності трьох стадій: "запис" (початковий стан – initialization), "обчислення" (унітарні перетворення початкового стану), "вивід" (вимірювання, проектування кінцевого стану).



Рис. 1. Схематичне зображення квантового процесора

1. Математичний опис станів квантових бітів регістра квантового процесора. Квантовий процесор оперує квантовими бітами (q -бітами, кубітами – quantum bits) даних – станами квантової системи з двома квантовими рівнями, які сукупно утворюють нормований ортогональний базис $\{|0\rangle, |1\rangle\}$.

Основною відмінністю квантового біта є його здатність утворювати когерентну суперпозицію базисних квантових станів, яка математично формалізується у вигляді вектора стану – хвильової функції

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

де комплексні числа α та β задовольняють умові нормування

$$|\alpha|^2 + |\beta|^2 = 1,$$

де $|\alpha|^2$ – ймовірність появи базисного стану $|0\rangle$, а $|\beta|^2$ – ймовірність появи базисного стану $|1\rangle$. Тобто, q -біт перебуває одночасно у базисних станах $|0\rangle$ та $|1\rangle$.

Вимірювання квантового стану $|\psi\rangle$ кубіта полягає в обчисленні коефіцієнтів розкладу, тобто, у проектуванні вектора стану на базисні орти – вектори базисних станів:

$$\alpha = \langle 0|\psi\rangle, \quad \beta = \langle 1|\psi\rangle.$$

Загалом квантовий стан кубіта геометрично можна зобразити стрілкою на сфері Блоха, як наведено на рис. 2.

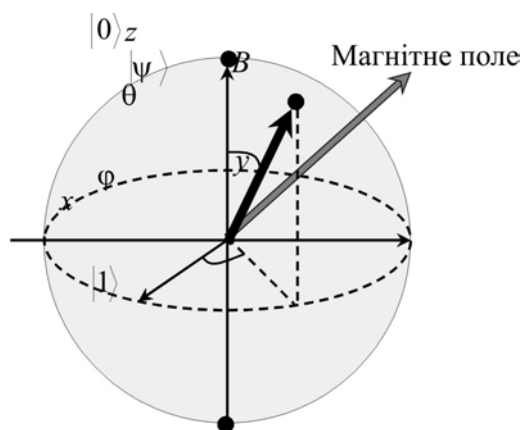


Рис. 2. Довільний квантовий стан $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ кубіта на сфері Блоха

Для реалізації багатокубітного (повномасштабного) квантового процесора (регістра квантового процесора) використовується сімейство q -бітів. Регістр квантового процесора принципово відрізняється від регістра класичного процесора. Розмір простору станів сукупності класичних бітів регістра класичного процесора лінійно зростає за збільшення кількості бітів

$$\dim(X_1 \times X_2 \times X_3 \times \dots \times X_L) = \dim(X_1) + \dim(X_2) + \dim(X_3) + \dots + \dim(X_L),$$

де $X_1, X_2, X_3, \dots, X_L$ – стани відповідно першого, другого, третього, ..., L -го класичних бітів, $\times$ – декартовий добуток.

Розмір простору станів сукупності квантових бітів регістра квантового процесора експоненційно зростає із збільшенням кількості q -біт

$$\dim(H_1 \otimes H_2 \otimes H_3 \otimes \dots \otimes H_L) = \dim(H_1) \cdot \dim(H_2) \cdot \dim(H_3) \cdot \dots \cdot \dim(H_L),$$

де $H_1, H_2, H_3, \dots, H_L$ – стани відповідно першого, другого, третього, ..., L -го квантових бітів, $\otimes$ – тензорний добуток.

Тобто, довільний квантовий стан квантового регістра, що складається із L q -бітова на відміну від класичного регістра з аналогічним числом класичних бітів, може перебувати у будь-якій когерентній суперпозиції із 2^L булевими станами і математично описується вектором стану в 2^L -вимірному комплексному гільбертовому просторі.

Істотною властивістю регістра квантового процесора протягом виконання над ним унітарних перетворень (квантових обчислень) є когерентна інтерференція між суперпозиціями, що являє собою квантовий паралелізм. Саме квантовий паралелізм є головною відмінністю та перевагою квантових обчислень над класичними обчисленнями.

Якщо розглянути двокубітний регістр, то базисні орти матимуть вигляд:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle,$$

а їх квантовий стан описуватиметься

$$|\psi\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,$$

де добутки комплексних чисел $\alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2$ задовольняють умову нормування $|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 = 1$ й $|\alpha_1\alpha_2|^2, |\alpha_1\beta_2|^2, |\beta_1\alpha_2|^2, |\beta_1\beta_2|^2$ – відповідно ймовірності базисних станів $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

Слушно відзначити, що двокубітний регістр квантового процесора може перебувати у запутаних станах (entangled states), наприклад,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

це стосується і трикубітного регістра – запутані стани, наприклад,

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle), \dots$$

та загалом L кубітного регістра.

2. Неможливість використання класичної статистичної моделі для математичного опису стадії вимірювання стану регістра квантового процесора й можливість використання квантової статистичної моделі. Визначальною особливістю квантового процесора є квантова випадкова природа вихідних даних, що є діаметрально протилежним порівняно з вихідними даними класичного процесора, які є детермінованими; крім цього, стохастичне функціонування квантового процесора, зокрема, стадія вимірювання – проектування кінцевого стану, не може бути математично формалізована у вигляді класичної статистичної моделі – аксіоматичної теорії:

Аксіома 1. Кожній випадковій події A (що є підмножиною простору елементарних випадкових подій Ω) поставлено у відповідність невід'ємне число $prob(A)$, що називається її ймовірністю.

Аксіома 2. $prob(\Omega) = 1$.

Аксіома 3. Якщо випадкові події $A_1, A_2, A_3, \dots, A_n$ є попарно несумісними ($A_i \cap A_j = \emptyset$, коли $i \neq j$, $i, j = \overline{1, n}$), то

$$prob(A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n) = prob(A_1) + prob(A_2) + prob(A_3) + \dots + prob(A_n).$$

Причиною того, що стадія приготування і вимірювання не описуються класичною статистичною моделлю є те, що стан регістра квантового процесора не може бути представлений у вигляді розподілу ймовірностей $prob(d\omega)$ на просторі елементарних випадкових подій Ω .

Робота квантового процесора, зокрема стадія вимірювання, математично формалізується у вигляді квантової статистичної моделі – теорії унітарних операторів у гільбертовому просторі.

Якщо регістр квантового процесора містить L q -бітів, то дані на його виході можуть перебувати у довільному квантовому стані

$$|\psi\rangle = \sum_{i=0}^{2^L-1} \alpha_i |e_i\rangle, \quad (1)$$

де ортонормовані базисні стани мають вигляд $|e_0\rangle = |00 \dots 00\rangle$, $|e_1\rangle = |00 \dots 01\rangle$, $|e_2\rangle = |00 \dots 10\rangle$, $|e_3\rangle = |00 \dots 11\rangle, \dots, |e_{2^L-1}\rangle = |11 \dots 11\rangle$; $\alpha_i \in \mathbb{C}$, $i = \overline{0, 2^L-1}$,

$$\sum_{i=0}^{2^L-1} |\alpha_i|^2 = 1.$$

Сукупність Ψ всіх можливих квантових станів (1) L q -бітового регістра квантового процесора є опуклим простором хвильових функцій (векторним простором векторів станів над полем комплексних чисел, у якому задано скалярний добуток векторів станів).

Вимірювання даних регістра q -процесора – це афінне відображення

$$\Psi \rightarrow \left\{ \left(\Omega_{|\psi\rangle}, \sigma_{|\psi\rangle} - \text{алгебра}, \text{prob}_{|\psi\rangle} \right) : |\psi\rangle \in \Psi \right\}$$

де Ψ – випуклий комплексний гільбертовий простір векторів станів регістра квантового процесора над полем комплексних чисел; $\left\{ \left(\Omega_{|\psi\rangle}, \sigma_{|\psi\rangle} - \text{алгебра}, \text{prob}_{|\psi\rangle} \right) : |\psi\rangle \in \Psi \right\}$ – множина ймовірнісних просторів кожен з яких відповідає конкретному стану $|\psi\rangle$ регістра квантового процесора: $\Omega_{|\psi\rangle}$ – простір елементарних випадкових подій, $\sigma_{|\psi\rangle}$ – алгебра – алгебра підмножин $\Omega_{|\psi\rangle}$, $\text{prob}_{|\psi\rangle}$ – ймовірнісна міра, яка визначена на $\sigma_{|\psi\rangle}$ – алгебрі.

3. Математичний опис стадії обчислення квантового процесора.

Як було зазначено вище квантова статистична модель є математичною формалізацією стадії вимірювання даних регістра q -процесора і лише опосередковано торкається стадії унітарних перетворень, тобто квантових обчислень, початкового стану регістра. Однак з алгоритмічної точки зору, саме стадія унітарних перетворень квантового стану регістра q -процесора є найбільш значимою. Для формалізації стадії унітарних перетворень над квантовим станом регістра q -процесора використовуються комплексний гільбертовий простір H , якому належить сукупність $\Psi = \{|\psi\rangle\}$ векторів станів (хвильових функцій) регістра квантового процесора, та сукупність $\cup = \{U\}$ унітарних операторів, тобто таких операторів, що задовольняють умову

$$\| |\psi\rangle \|_{H_1} = \| U|\psi\rangle \|_{H_2}.$$

Слушно відзначити, що сукупність $\cup = \{U\}$, яка діє у комплексному гільбертовому просторі H утворює некомутативну групу. Разом – $\Psi = \{|\psi\rangle : |\psi\rangle \in H\}$ та $\cup = \{U\}$ утворюють квантову мережу (quantum network), в якій унітарні оператори U називаються квантовими логічними елементами (КЛЕ – quantum gates). Унітарні перетворення (квантові обчислення) над квантовим станом регістра квантового процесора представляють обертання вектора квантового стану у комплексному гільбертовому просторі.

3.1. Математичний опис однокубітних квантових логічних елементів (однокубітних унітарних операторів). До найпростіших КЛЕ належать однокубітні КЛЕ, які аналогічно багатокубітним КЛЕ, математично формалізуються у вигляді матриць, а їх дія на квантовий стан регістра квантового процесора графічно видається квантовою мережею.

Серед однокубітних КЛЕ використовують:

- однокубітний унітарний оператор Адамара (Hadamard)

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

дія якого на один квантовий біт зображується квантовою мережею (рис. 3)

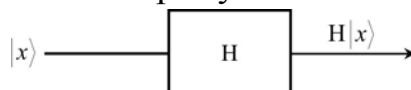


Рис. 3. Вигляд квантової мережі, що зображує дію оператора Адамара H
та аналітично видається у вигляді

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle);$$

- однокубітний унітарний оператор зміни фази

$$\Phi(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\varphi) \end{pmatrix}$$

дія якого на один квантовий біт зображується квантовою мережею (рис. 4)

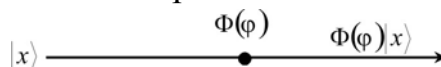


Рис. 4. Вигляд квантової мережі, що зображує дію оператора зміни фази $\Phi(\varphi)$
та аналітично видається у вигляді

$$|0\rangle \rightarrow |0\rangle, |1\rangle \rightarrow \exp(i\varphi)|1\rangle;$$

- однокубітний унітарний оператор (beam-splitter)

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

дія якого на один квантовий біт зображується квантовою мережею (рис. 5)

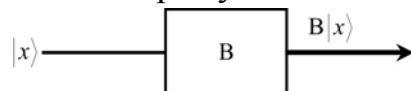


Рис. 5. Вигляд квантової мережі, що зображує дію оператора (beam-splitter) B
та аналітично видається у вигляді

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(i|0\rangle + |1\rangle), |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle).$$

Пари операторів $(H, \Phi(\varphi))$ та $(B, \Phi(\varphi))$ утворюють повні зв'язки, тобто з них можна отримати довільні однокубітні КЛЕ.

3.2. Математичний опис двокубітного та багатокубітних квантових логічних елементів. Реалізація довільної булевої операції за допомогою лише сімейства $\cup = \{U\}$ унітарних однокубітних операторів не можлива. Потрібно використовувати двокубітний унітарний оператор контрольоване заперечення (**XOR** або **CNOT – Controlled-NOT**). Двокубітний унітарний оператор контрольоване заперечення діє в чотиривимірному комплексному векторному просторі станів двокубітового регістра квантового процесора з ортонормованим базисом $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Унітарний оператор контрольоване заперечення

$$\mathbf{XOR} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

дія якого на двокубітовий квантовий регістр зображається квантовою мережею, що наведена на рис. 6.

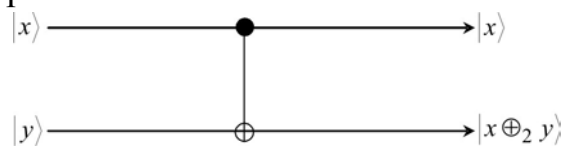


Рис. 6. Вигляд квантової мережі, що зображає дію унітарного двокубітного оператора XOR; • – керуючий q -біт, $\oplus$ – керований q -біт

Та аналітично у вигляді

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle.$$

Двох однокубітних унітарних операторів H і $\Phi(\varphi)$, або V і $\Phi(\varphi)$ та двокубітного унітарного оператора **XOR** достатньо, щоб побудувати довільний унітарний оператор, який діє в 2^L -вимірному комплексному векторному просторі станів L -кубітового регістра квантового процесора з ортонормованим базисом $|00\dots 00\rangle, |00\dots 01\rangle, |00\dots 10\rangle, \dots, |11\dots 11\rangle$.

Серед множини унітарних операторів, які діють на L q -бітах регістра квантового процесора, найбільшого застосування набули:

- квантовий унітарний оператор Уолша-Адамара W , який застосовує квантовий унітарний оператор Адамара H до всіх L q -бітів квантового регістра, створюючи суперпозицію 2^L чисел у двійковій системі числення від 0 до $2^L - 1$, має вигляд:

$$W|000\dots 0_L\rangle = (H_1 \otimes H_2 \otimes H_3 \otimes \dots \otimes H_L)|000\dots 0_L\rangle = \\ = \frac{1}{\sqrt{2}}((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2}} \sum_{x=0}^{2^L-1} |x\rangle.$$

Його квантову мережу наведено на рис. 7.

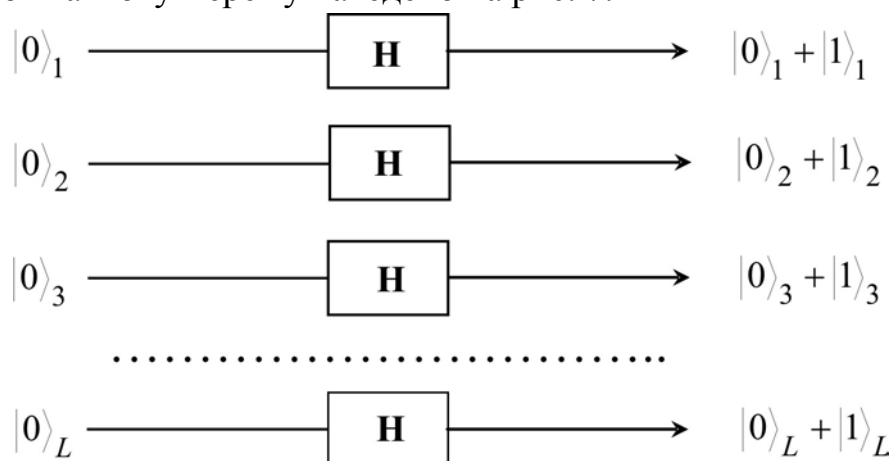


Рис. 7. Вигляд квантової мережі, що зображає дію оператора W

- квантовий унітарний оператор **Controlled-Controlled NOT**, дію якого зображено квантовою мережею, що наведена на рис. 8.

4. Об'єднання математичних описів стадій запису та обчислення в єдину математичну модель. Вище наведені математичні описи, що математично формалізують роботу КЛЕ, разом із векторами станів регістра квантового процесора утворюють математичну модель стадій "запису" та "обчислення" у вигляді

$$\langle \Psi, D, U \rangle,$$

де Ψ – випуклий комплексний гільбертовий векторний простір векторів станів реєстра квантового процесора над полем комплексних чисел, $D = D(\psi, f(t))$ – динамічна еволюція квантового стану реєстра квантового процесора, $\psi \in \Psi$ (наприклад, початковий стан – initial state), $f(t) \subset U$ (впорядкована підмножина КЛЕ, що належить унітарному комплексному векторному простору U над полем комплексних чисел).

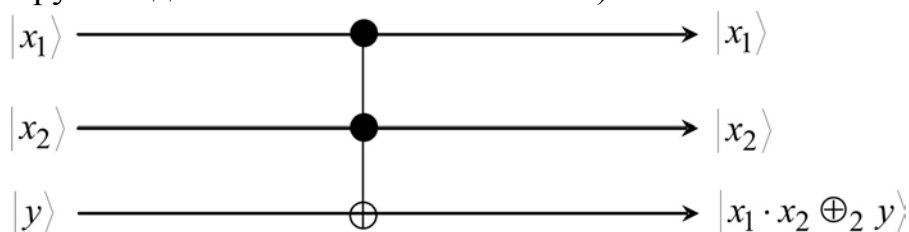


Рис. 8. Вигляд квантової мережі, що зображує дію оператора *Controlled-Controlled NOT*

Висновки. Висвітлено основи математичного формалізму функціонування квантового процесора, що становить основу розроблення нових сучасних квантових інформаційних систем.

Література

1. **Оснoвы квантовых вычислений** / Э. Стин // Квантовые компьютеры и квантовые вычисления. – 2001. – Т.2, № 1. – С. 3-24.
2. **Валиев К.А.** Квантовые компьютеры: надежды и реальность / К.А. Валиев, А.А. Кокин. – Иркутск : Изд-во РХД, 2001. – 352 с.
3. **Войтович І.Д.** Перспективи квантових обчислень з використанням надпровідності / І.Д. Войтович, В.М. Корсунський // Математичні машини і системи. – 2008. – № 4. – С. 23-56.
4. **Крохмальський Т.** Квантові комп'ютери: основи й алгоритми (короткий огляд) / Т. Крохмальський // Журнал фізичних досліджень. Ін-ут фізики конденсованих систем НАН України. – 2004. – Т.8, № 1. – С. 1-15.

УДК 336.71

Аспір. К.О. Ільїна¹ – Львівський НУ ім. Івана Франка

КАТЕГОРІАЛЬНИЙ АПАРАТ ІННОВАЦІЙНОЇ ТЕОРІЇ ЯК ФУНДАМЕНТ ЗАПРОВАДЖЕННЯ ІННОВАЦІЙНО-ІНВЕСТИЦІЙНОЇ МОДЕЛІ РОЗВИТКУ В УКРАЇНСЬКУ ЕКОНОМІЧНУ СИСТЕМУ

Систематизовано підходи вітчизняних і зарубіжних вчених до основних категорій інноваційної теорії. Запропоновано визначення понять "новація", "інновація", "інноваційний процес". Здійснено поділ інноваційного процесу на структурні елементи. Пояснено суть структурних елементів інноваційного процесу.

Ключові слова: новація, інновація, інноваційний процес, дослідження, комерціалізація

Post-graduate K.O. Il'ina – L'viv NU named after Ivan Franko

Category of innovative theory as foundation of introduction of innovative investment model of development in the Ukrainian economic system

The basic categories of innovative theory of Ukrainian and foreign scientists are systematized. Determination of concepts of innovation, innovation, innovative process is

¹ Наук. керівник: проф. М.І. Крупка, д-р техн. наук – Львівський НУ ім. Івана Франка