УДК 002:651.928(083.73):621.039.58
Проф. В.М. Максимович, д-р техн. наук;
доц. О.І. Гарасимчук, канд. техн. наук; асист. Ю.М. Костів;
аспір. М.М. Мандрона – НУ "Львівська політехніка", м. Львів

МЕТОДИКА ОПТИМІЗАЦІЇ ПАРАМЕТРІВ ГЕНЕРАТОРІВ ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОСЛІДОВНОСТЕЙ, ПОБУДОВАНИХ НА ОСНОВІ ЛІНІЙНИХ КОНГРУЕНТНИХ ГЕНЕРАТОРІВ

Розроблено узагальнену методику, яка дає змогу досліджувати параметри вихідного сигналу генераторів пуассонівських імпульсних послідовностей. Цю методику можна використовувати при оптимізації параметрів генераторів псевдовипадкових чисел, які є основою генераторів пуассонівських імпульсних послідовностей. Подано результати моделювання генераторів пуассонівських імпульсних послідовностей із різними параметрами лінійного конгруентного генератора.

Ключові слова: генератори пуассонівських імпульсних послідовностей, лінійні конгруентні генератори, генератори псевдовипадкових чисел.

Генератори випадкових і псевдовипадкових імпульсних послідовностей широко використовують у криптографії, в імітаційному моделюванні, у вимірювальній техніці, засобах зв'язку, радіолокації тощо. Одне з важливих місць серед таких генераторів займають генератори пуассонівських імпульсних послідовностей (ГПІП), які залежно від мети і сфери застосування, можуть бути реалізовані як апаратними, так і програмними засобами.

У роботі **[**1, 2**]** запропоновано узагальнену структуру ГПІП (рис. 1), що складається з генератора псевдовипадкових чисел (ГПВЧ), схеми порівняння (СП) і логічного елемента (І).

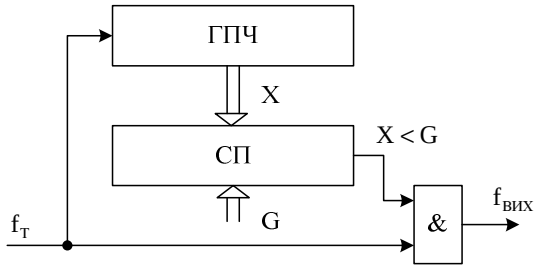


Рис. 1. Узагальнена структура ГПІП

Тактові імпульси проходять на вихід ГПІП, якщо число X на виході ГПВЧ менше від керуючого коду G. Середня частота вихідних імпульсів генератора визначається рівнянням

$$f_{ВИХ} = \frac{\mathrm{G}}{\mathrm{X}_{\max}} f_T , \qquad (1)$$

де: $X_{\max}$ – максимальне значення X; f_T – частота повторення тактових імпульсів.

Постановка проблеми. Якість ГПІП, тобто відповідність статистичного розподілу в часі вихідних імпульсів пуассонівському закону, залежить від вибору ГПЧ. У роботах **[**1-3**]** розглянуто переваги ГПІП, в основі яких є структура,

наведена на рис. 1, і досліджено деякі їх характеристики. Однак при цьому не були вирішені такі задачі:

- вибір оптимальної кількості розрядів ГПЧ для забезпечення необхідних параметрів вихідного сигналу ГПІП при розв'язанні конкретних прикладних задач;
- взаємозв'язок параметрів ГПВЧ і діапазону значень керуючого коду G з частотно-часовими параметрами вихідного сигналу;
- створення узагальненої методики дослідження параметрів ГПІП незалежно від вибору типу ГПВЧ.

З метою розв'язання цих задач ми створили узагальнену методику дослідження параметрів вихідного сигналу ГПІП. У цій роботі її використано при побудові ГПВЧ за алгоритмом роботи лінійного конгруентного генератора. Виклад основного матеріалу. Потік вхідних імпульсів ГПІП розбиваємо на n однакових груп, кожна з яких складається з $i_{\max}$ імпульсів (рис. 2). Максимальну кількість груп позначимо $n_{\max}$, а проміжок часу, що їм відповідає – T_B. Групам вхідних імпульсів відповідають групи вихідних імпульсів з числом імпульсів $k_1, k_2, \ldots, k_{n_{\max}}$.

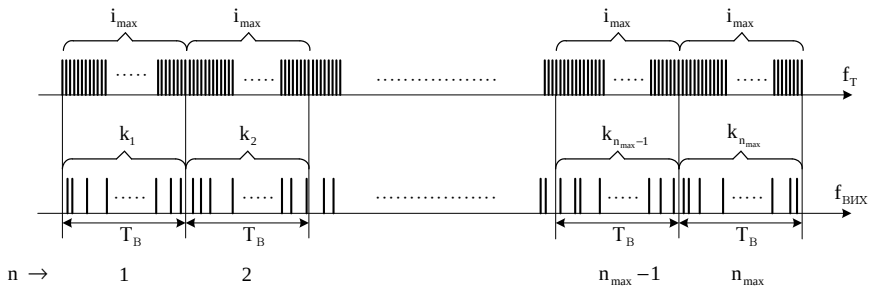


Рис. 2. Розбиття вхідних і вихідних імпульсних потоків на групи

Враховуючи рівняння (1), середню кількість вихідних імпульсів у групі можна визначити так:

$$k_C = \frac{G}{X_{\max}} i_{\max} . \qquad (2)$$

Під час дослідження статистичних параметрів вихідної імпульсної послідовності ГПІП необхідно:

- вибрати математичний апарат для оцінки статистичних характеристик імпульсного потоку, з урахуванням його розбиття на групи (рис. 2);
- вибрати оптимальні значення $i_{\max}$ і $n_{\max}$ залежно від кількості розрядів (діапазону значень вихідного коду) вибраного ГПВЧ.

Для оцінки статистичних характеристик імпульсного потоку на його відповідність пуассонівському закону розподілу можна скористатись такими залежностями. Якщо імпульсний випадковий потік підпорядковується закону Пуассона, то імовірність появи рівно k імпульсів за час T_B описується формулою **[**4-6**]**

$$\mathrm{P_k}(k_C, \mathrm{T_B}) = \frac{(\mathrm{k_C} \cdot \mathrm{T_B})^k}{k!} e^{-\mathrm{k_C} \cdot \mathrm{T_B}} . \qquad (3)$$

Математичне сподівання і дисперсія випадкової величини, розподіленої за законом Пуассона, збігаються і дорівнюють

$$M(k) = D(k) = k_C \cdot T_B . \quad (4)$$

Кількість імпульсів пуассонівського імпульсного потоку, яка зафіксована за час T_B:

а) з надійною ймовірністю p=0,68 знаходиться у межах **[**9**]**

$$k_C - \sqrt{k_C} < k < k_C + \sqrt{k_C} ; \quad (5)$$

б) з надійною ймовірністю p=0,95 – у межах

$$\mathrm{k_C} - 2\sqrt{\mathrm{k_C}} < \mathrm{k} < \mathrm{k_C} + 2\sqrt{\mathrm{k_C}} ; \quad (6)$$

в) з надійною ймовірністю p=0,997 – у межах

$$\mathrm{k_C} - 3\sqrt{\mathrm{k_C}} < \mathrm{k} < \mathrm{k_C} + 3\sqrt{\mathrm{k_C}} . \quad (7)$$

Одним із відомих оціночних методів для тестування псевдовипадкових послідовностей з заданим законом розподілу є також критерій χ^2 **[**5-9**]**.

У цій роботі для створення узагальненої методики дослідження параметрів ГПІП ми будемо використовувати тільки вираз (6), вважаючи, що використання інших математичних співвідношень і тестів може бути лише уточнюючим фактором. Для обґрунтування вибору оптимальних значень $i_{\max}$ і $n_{\max}$ конкретизуємо тип і параметри ГПВЧ. Нехай, в якості останнього використано лінійний конгруентний генератор, що працює відповідно до рекурентного рівняння

$$X_{i+1} = (aX_i + b) \bmod m . \quad (8)$$

Для забезпечення максимально можливого періоду повторення значень $X_i - m$, необхідно, щоб значення a, b і m відповідали певним вимогам **[**9**]**. Для подальших досліджень виберемо: $a = 1366$, $b = 150889$, $m = 714025$. Конкретизуємо також, для початку, значення керуючого коду – $G = 10000$.

У табл. 1 для різних значень $i_{\max}$ визначено середньотеоретичні значення k_C – кількості вихідних імпульсів ГПІП на інтервалі T_B. При цьому використовували залежність

$$k_C = \frac{G}{m-1} i_{\max} , \quad (9)$$

отриману з (2), оскільки при досягненні максимально можливого періоду повторення ГПЧ – $X_{\max} = m - 1$. Тут також наведено значення $\mathrm{k_{H\_95}}$ і $\mathrm{k_{B\_95}}$, що відповідають нижній і верхній межам подвійної нерівності (6).

Табл. 1. Теоретичні параметри ГПІП при a = 1366, b = 150889, m = 714025, G = 10000

$i_{\max}$	k_C	$\mathrm{k_{H\_95}}$	$\mathrm{k_{B\_95}}$
100	1.40	-0.97	3.77
1000	14.01	6.52	21.49
10000	140.05	116.38	163.72
100000	1400.51	1325.67	1475.36
1000000	14005.13	13768.44	14241.82

Результати моделювання ГПІП з визначеними вище параметрами наведено у табл. 2.

Табл. 2. Результати моделювання ГПІП при a = 1366, b = 150889, m = 714025, G = 10000

$i_{\max}$	k_{95}		
	$n_{\max} = 100$	$n_{\max} = 1000$	$n_{\max} = 10000$
100	4	49	515
1000	3	44	419
10000	2	15	146
100000	1	7	75
1000000	0	0	0

У табл. 2, для різних значень $i_{\max}$ і $n_{\max}$ внаслідок моделювання, визначено скільки значень k вийшли за межі (6) – k_{95}. Теоретично, в ідеальному випадку, значення k_{95} для $n_{\max} = 100$ повинно дорівнювати 5, для $n_{\max} = 1000$ – 50, а для $n_{\max} = 10000$ – 500.

Результати, які наведені у табл. 1, засвідчують, що значення k_{95} наближаються до теоретичних, якщо виконується умова

$$i_{\max} \cdot n_{\max} < m , \quad (10)$$

що підтверджує висновки, виведені у роботі **[**2**]**.

Для подальших досліджень необхідно конкретизувати значення $i_{\max}$ і $n_{\max}$. Значення $n_{\max}$ повинно бути достатньо великим, щоб забезпечити задовільну статистику для визначення k_{95}, але не перевершувати ті значення, які б з урахуванням (10) призвели до зменшення $i_{\max}$ і, таким чином, до зменшення статистичної точності визначення окремих значень k.

Проведені дослідження показали, що такими значеннями, з урахуванням виразу (10), можуть бути:

$$n = 1000 , \; i_{\max} = Int\left(\frac{m}{n_{\max}}\right). \quad (11)$$

Параметри ГПІП мають бути досліджені за різних значень керуючого коду G. При цьому необхідно визначити межі значень G, за яких статистичні параметри вихідного імпульсного потоку генератора є задовільними.

У цій роботі нижню межу G визначено за мінімальним значенням k_C, при якому за допомогою виразу (6) можна проводити статистичний аналіз із задовільною точністю. Якщо прийняти $k_{C_{\min}} = 10$, тоді з (9) отримаємо

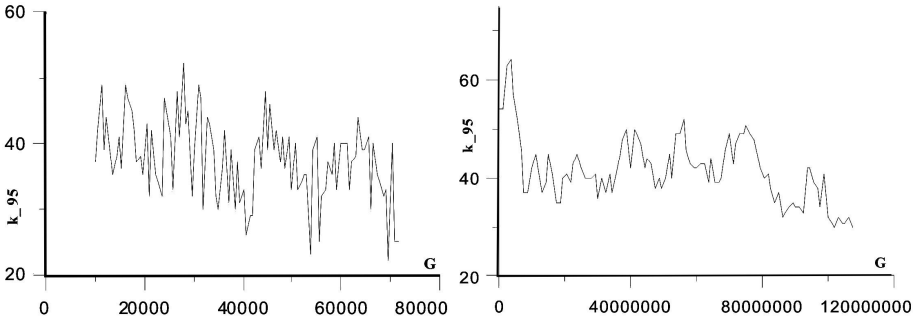
$$G_{\min} = \frac{k_{C_{\min}}(m-1)}{i_{\max}} = \frac{10(m-1)}{i_{\max}} . \quad (12)$$

Зрозуміло, що, в разі потреби, повинні бути проведені додаткові дослідження у випадку $G_{\min} = 1$, з використанням іншого математичного апарату, зокрема виразів (3), (4) і критерію χ^2.

Верхня межа керуючого коду визначається у процесі моделювання за результатами оцінки статистичних параметрів вихідного сигналу на відповідність пуассонівському закону розподілу. Внаслідок виконання попередніх досліджень булу прийнято

$$G_{\max} = 0.1 \cdot m. \qquad (13)$$

На рис. 3, *а* наведено результати моделювання ГПІП при $a = 1366$, $b = 150889$, $m = 714025$ і керуючому коді, що змінюється в межах заданих рівняннями (12), (13). З допомогою наведеного графіка можуть бути уточнені прийнятні межі значень керуючого коду. При цьому потрібно керуватись максимально допустимим відхиленням значень k_{95} від теоретично визначеного, в цьому випадку від числа 50, оскільки $n_{\max} = 1000$. Максимально допустимі відхилення повинні визначатись, своєю чергою, залежно від конкретних прикладних задач, що вирішуються з допомогою ГПІП.



а) б)

Рис. 3. Результати моделювання ГПІП при зміні G:
а) a = 1366, b = 150889, m = 714025; б) a = 105, b = 12345, m = 2^{30}

Наступним кроком розробленої методики є визначення частотно-часових параметрів вихідного сигналу ГПІП. Такі параметри для випадку коли $a = 1366$, $b = 150889$, $m = 714025$, для різних значень тактової частоти f_T, наведено в табл. 3.

Табл. 3. Частотно-часові параметри ГПІП при a = 1366, b = 150889, m = 714025

f_T[Гц]	$f_{ВИХ_{\min}}$[Гц]	$f_{ВИХ_{\max}}$[Гц]	$\Delta f_{ВИХ}$[Гц]	$T_{\max}$[с]
1000.0	14.01	100.0	0.0014	714.0250
10000.0	140.06	1000.0	0.0140	71.4025
100000.0	1400.56	10000.0	0.1401	7.1402
1000000.0	14005.60	100000.0	1.4005	0.7140
10000000.0	140056.02	1000000.0	14.0051	0.0714

Тут $f_{ВИХ_{\min}}$, $f_{ВИХ_{\max}}$, $\Delta f_{ВИХ}$ – середні значення мінімальної, максимальної і кроку зміни вихідної частоти, визначені з рівнянь:

$$f_{ВИХ_{\min}} = \frac{G_{\min}}{m} f_T,\ f_{ВИХ_{\max}} = \frac{G_{\max}}{m} f_T,\ \Delta f_{ВИХ} = \frac{1}{m} f_T; \qquad (14)$$

де: $T_{\max}$ – час, що відповідає $n_{\max}$ групам тактових і вихідних імпульсів (рис. 2):

$$T_{\max} = \frac{i_{\max} \cdot n_{\max}}{f_T}. \qquad (15)$$

При використанні ГПІП для імітації вихідних сигналів дозиметричних детекторів **[4]**, на основі даних табл. 3 можна отримати відповідні параметри радіаційного випромінювання (табл. 4).

Табл. 4. Параметри вихідних сигналів дозиметричних детекторів при їх імітації за допомогою ГПІП (a = 1366, b = 150889, m = 714025)

f_T[Гц]	$T_{\max}$[с]	$P_{\min}[мкР/год]$	$P_{\max}[мкР/год]$	$\Delta P[мкР/год]$
1000.0	714.0250	700.28	5000.0	0.0700
10000.0	71.4025	7002.80	50000.0	0.7003
100000.0	7.1402	70028.01	500000.0	7.0026
1000000.0	0.7140	700280.11	5000000.0	70.0256
10000000.0	0.0714	7002801.12	50000000.0	700.2556

Тут $P_{\min}$, $P_{\max}$, ΔP – середні значення мінімальної, максимальної і кроку зміни потужності експозиційної дози, визначені з рівнянь:

$$P_{\min} = \frac{f_{ВИХ_{\min}}}{\gamma},\ P_{\max} = \frac{f_{ВИХ_{\max}}}{\gamma},\ \Delta P = \frac{\Delta f_{ВИХ}}{\gamma}, \qquad (16)$$

де γ – чутливість дозиметричного детектора. У наведеному прикладі прийняте значення $\gamma = 0.02\left[\frac{Гц}{мкР/год}\right]$.

На рис. 3, *б* і в табл. 5 і 6 наведено результати дослідження ГПІП з лінійним конгруентним ГПВЧ, при $a = 105$, $b = 12345$, $m = 2^{30}$.

Табл. 5. Частотно-часові параметри ГПІП при a = 105, b = 12345, m = 2^{30}

f_T[Гц]	$f_{ВИХ_{\min}}$[Гц]	$f_{ВИХ_{\max}}$[Гц]	$\Delta f_{ВИХ}$[Гц]	$T_{\max}$[с]
1000.0	0.0093	100.0	0.00000093	1073741.8240
10000.0	0.0931	1000.0	0.00000931	107374.1824
100000.0	0.9313	10000.0	0.00009313	10737.4182
1000000.0	9.3132	100000.0	0.00093132	1073.7418
10000000.0	93.1323	1000000.0	0.00931323	107.3742

Табл. 6. Параметри вихідних сигналів дозиметричних детекторів при їх імітації за допомогою ГПІП (a = 105, b = 12345, m = 2^{30})

f_T[Гц]	$T_{\max}$[с]	$P_{\min}[мкР/год]$	$P_{\max}[мкР/год]$	$\Delta P[мкР/год]$
1000.0	1073741.8240	0.47	5000.0	0.00004657
10000.0	107374.1824	4.66	50000.0	0.00046566
100000.0	10737.4182	46.57	500000.0	0.00465661
1000000.0	1073.7418	465.66	5000000.0	0.04656613
10000000.0	107.3742	4656.62	50000000.0	0.46566129

Висновок. Розроблена методика може бути використана для оптимізації параметрів генераторів пуассонівських імпульсних послідовностей з урахуванням їх прикладного застосування.

Література

1. Гарасимчук О.І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О.І. Гарасимчук, В.М. Максимович // Вісник Національного університету "Львівська політехніка". – Сер.: "Комп'ютерна інженерія та інформаційні технології". – 2004. – № 521. – С. 17-23.

2. Гарасимчук О.І. Генератори тестових імпульсних послідовностей для дозиметричних пристроїв / О.І. Гарасимчук, В.Б. Дудикевич, В.М. Максимович, Р.Т. Смук // Вісник Національного університету "Львівська політехніка". – Сер.: "Теплоенергетика. Інженерія довкілля. Автоматизація". – 2004. – № 506. – С. 187-193.

3. Максимович В.М. Оптимізація параметрів генератора М-послідовностей як структурного елемента генератора пуассонівської імпульсної послідовності / В.М. Максимович, О.І. Гарасимчук, Ю.М. Костів // Вісник Національного університету "Львівська політехніка". – Сер.: "Автоматика, вимірювання та керування". – 2011. – № 695. – С. 46-51.

4. Бендат Дж. Прикладной анализ случайных даных / Дж. Бендат, А. Пирсол. – М. : Изд-во "Мир", 1989. – 540 с.

5. Бобнев М.П. Генерирование случайных сигналов / М.П. Бобнев. – Изд. 2-ое, [перераб. и доп.]. – М. : Изд-во "Энергия", 1971. – 239 с.

6. Орнатский П.П. Теоретические основы информационно-измерительной техники : учебник [для студ. ВУЗов] по спец. "Информ.-изм. техника". – Изд. 2-ое, [перераб. и доп.]. – К. : Вид-во "Вища шк.", 1983. – 455 с.

7. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : Изд-во КУДИЦ-ОБРАЗ, 2003. – 240 с.

8. Кнут Д. Искусство программирования для ЭВМ. – В 3-х т. Получисленные алгоритмы : пер. с англ. – М. : Изд-во "Мир", 1977.

9. Бобало Ю.Я. Методи і засоби опрацювання вихідних сигналів дозиметричних детекторів : монографія / Ю.Я. Бобало, В.Б. Дудикевич, В.М. Максимович, В.О. Хорошко, А.М. Бісик, Р.Т. Смук, Ю.Б. Сторонський. – Львів : Вид-во НУ "Львівська політехніка", 2009. – 200 с.

Максымовыч В.Н., Гарасымчук О.И., Костив Ю.М., Мандрона М.М.

Методика оптимизации параметров генераторов пуассоновских импульсных последовательностей, построенных на основе линейных конгруэнтных генераторов

Разработана обобщенная методика, позволяющая исследовать параметры выходного сигнала генераторов пуассоновских импульсных последовательностей. Данная методика может использоваться при оптимизации параметров генераторов псевдослучайных чисел, которые являются основой генераторов пуассоновских импульсных последовательностей. Представлены результаты моделирования генераторов пуассоновских импульсных последовательностей с различными параметрами линейного конгруэнтного генератора.

Ключевые слова: генераторы пуассоновских импульсных последовательностей, линейные конгруэнтные генераторы, генераторы псевдослучайных чисел.

Maksymovych V.M., Garasymchuk O.I., Kostiv Y.M., Mandrona M.M.

Methods of optimization parameters of Poisson pulse sequences generators constructed on the basis of linear congruent generators

The generalized method, that allow to investigate parameters of Poisson pulse sequence generators output signal is work out. Method can be used for optimization of pseudorandom number generators parameters that are the basis of Poisson pulse sequence generators. The results of simulation of Poisson pulse sequence generator, with different parameters of linear congruent generator, are represented.

Keywords: Poisson pulse sequences generators, linear congruential generators, pseudorandom number generators.

УДК 378.1

Доц. О.Ю. Чмир, канд. фіз.-мат. наук; доц. О.О. Карабин, канд. фіз.-мат. наук – Львівський ДУ безпеки життєдіяльності

ГЕОМЕТРИЧНЕ ЗАСТОСУВАННЯ ПОДВІЙНОГО ІНТЕГРАЛА З ВИКОРИСТАННЯМ КОМАНД ПАКЕТУ MAPLE

Обгрунтовано доцільність поєднання сучасних інформаційних технологій та традиційних методів навчання під час викладання вищої математики студентам технічних спеціальностей. Наведено приклади реалізації розв'язування деяких задач з розділу "Інтегральне числення функцій багатьох змінних" засобами програмного пакету Maple. З'ясовано необхідність глибокої фундаментальної підготовки з вищої математики для оволодіння прийомами розрахунків програмними засобами, за допомогою яких розв'язування складних задач спрощується.

Ключові слова: інноваційні методи, програмні засоби навчання, інформаційні технології, область інтегрування.

Сучасне суспільство ставить високі вимоги до молодих фахівців, які завершили навчання у вищих навчальних закладах. Технічний прогрес значно випереджує сучасну національну освіту. У Національній доктрині розвитку освіти на чільному місці стоїть теза, що освіта є визначальним чинником політичної, соціально-економічної, культурної та наукової життєдіяльності суспільства. В Україні потрібно забезпечувати прискорений, випереджальний інноваційний розвиток освіти, а також створювати умови для розвитку, самоствердження та самореалізації особистості протягом життя **[**1**]**. Знання, здобуті в процесі навчання у вищій школі, повинні мати універсальний, фундаментальний характер. Особа – молодий фахівець використовуючи здобутий багаж знань, повинен вміти адаптуватись до нових умов. Цього можна досягнути лише здобуттям фундаментальних знань, з яких можна виділити все необхідне для своєї діяльності. Досягнути такого рівня знань можна завдяки впровадженню в навчальний процес освітніх технологій в поєднанні із традиційними методами навчання. У Національній доктрині розвитку освіти зазначено, що пріоритетом розвитку освіти є впровадження інформаційно-комунікаційних технологій, що забезпечують дальше вдосконалення навчально-виховного процесу, доступність та ефективність освіти, підготовку молодого покоління до життєдіяльності в інформаційному суспільстві **[**1**]**.

У педагогічній науці є дуже багато напрямів у дослідженні проблеми впровадження інноваційних технологій в навчальний процес. Багато досліджень спрямовані на проблеми інноваційних технологій в загальноосвітніх навчальних закладах. Проблема впровадження інформаційних технологій в навчальний процес вищої школи також не залишена поза увагою. Зокрема, в роботі **[**2**]** розглянуто суть поняття "інновація" і подано окремі інноваційні методи навчання у вищій школі, які стосуються лекційних занять. Проте інноваційні технології є неможливими без використання сучасних технічних і програмних засобів. Саме в роботах **[**3**]** та **[**4**]** порушена проблема створення високотехнологічного інформаційно-комунікаційного середовища, в якому має знаходитись сучасний студент. У роботі **[**3**]** визначено новий клас педагогічного програмного забезпечення математичних дисциплін – мобільне математичне середовище, основною складовою якого є обчислювальне ядро (математичний пакет). Таке