КОМП`ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 621.375.024

О.Д. АЗАРОВ, С.В. БОГОМОЛОВ

Вінницький національний технічний університет, Вінниця

ПРЕЦИЗІЙНІ БУФЕРНІ ПРИСТРОЇ НА БАЗІ ДВОТАКТНИХ СИМЕТРИЧНИХ СТРУКТУР

Анотація. Розглянуто методи структурно-функціональної організації прецизійних буферних пристроїв на базі двотактних симетричних структур. Наведено аналітичні співвідношення, що описують статичну передатну характеристику з урахуванням параметрів ядра схеми. Визначено складові, які призводять до появи похибки лінійності та показано способи її зменшення.

Ключові слова: прецизійність, буферний пристрій, похибки лінійності, структурна-функціональна організація, двотактна симетрична структура, двотактний підсилювач постійного струму.

Аннотация. Рассмотрены методы структурно-функциональной организации прецизионных буферных устройств на базе двухтактных симметричных структур. Приведены аналитические соотношения, описывающие статическую передаточную характеристику с учетом параметров ядра схемы. Определены составляющие, которые приводят к появлению погрешности линейности и показано способы ее уменьшения.

Ключевые слова: прецезионность, буферное устройство, погрешности линейности, структурно-функциональная организация, двухтактная симметрическая структура, двухтактный усилитель постоянного тока.

Annotation. The methods of structural and functional organization of precision buffer devices based on push-pull symmetric structures are considered. An analytical relation describing the static transfer characteristic parameters including kernel scheme. The composition, which lead to the appearance of linearity error and show how to reduce it.

Keyworlds: with precision, a buffer device,the error is linear, structural and functional organization, push-pull symmetric structure, push-pull dc amplifier.

Вступ

Буферні пристрої є аналоговими вузлами, що використовуються у багатьох електронних пристроях, зокрема, багаторозрядних системних АЦП і ЦАП, які у свою чергу входять до складу високоточних систем вимірювання, опрацювання та реєстрування сигналів [1-4]. Буферні пристрої по суті є підсилювачами потужності та призначені для узгодження опору генератора сигналу з опором навантаження [4]. При цьому буфер напруги (БН) виступає в ролі трансформатора опорів з високим вхідним та низьким вихідним опорами. Коефіцієнт передачі по напрузі БН дорівнює одиниці. Струм, який видається БН у навантаження, може бути набагато більший, ніж вхідний. Такі буферні пристрої називають повторювачами напруги [5]. Буфер струму (БС), наАвпаки, має низький вхідний та високий вихідний опори. Коефіцієнт передачі по струму БС, як правило, дорівнює одиниці і не залежить від опору навантаження.

Відомо багато різновидностей прецизійних буферних пристроїв, як за схемотехнічною організацією, так і призначенням. Найпоширенішою є побудова буферних пристроїв на базі операційних підсилювачів [1,2,4]. Проте, такий підхід обмежує їх швидкодію. Певний виграш при цьому має застосування для побудови ядра буферного пристрою двотактних складених емітерних повторювачів на біполярних транзисторах або двотактних структур на базі польових транзисторів.

Актуальність

У теперішній час особливу увагу привертають двотактні схеми буферних пристроїв. Вони здатні забезпечувати високу лінійність передатної характеристики і потрібну швидкодію [2, 4]. При цьому слід відзначити, що відомі схемотехнічні рішення буферних пристроїв за двотактною структурою, що забезпечують високу швидкодію і незначну нелінійність, є незбалансованими, мають велику похибку зсуву нуля і високий температурний дрейф. Водночас, матеріал, присвячений аналізу буферних пристроїв на базі двотактних симетричних структур, у науково-технічній літературі подається епізодично і є неструктурованим. Тому тема статті, присвячена побудові прецизійних буферних пристроїв на базі двотактних симетричних структур, є актуальною.

Мета

Аналіз методів структурно-функціональної організації прецизійних буферних пристроїв на базі двотактних симетричних структур з мінімізованими похибками лінійності і заданою швидкодією.

Постановка задач

1. Проаналізувати запропоновані методи структурно-функціональної організації прецизійних буферних пристроїв на базі двотактних симетричних структур.
2. Отримати аналітичні співвідношення похибок лінійності ядра буферного пристрою на основі двотактної симетричної структури.
3. Розглянути підхід, щодо підвищення навантажувальної здатності буферів напруги.

Розв'язання задач

Можна вказати декілька підходів, щодо побудови БН на базі двотактних симетричних структур.

При чому, незалежно від конкретної схемотехнічної реалізації, статична передатна характеристика цих пристроїв має загальну похибку:

$$\Delta U_{вих} = U_{вих} - U_{вх} \quad (1)$$

У свою чергу її можна розкласти на декілька складових, а саме на:

– похибку зсуву нуля $\Delta U_{зс0}$, причому $\Delta U_{зс0} = \Delta U_{вих}$, при $U_{вх} = 0$;

– похибку масштабу $\Delta U_{м}$, причому $\Delta U_{м} = U_{вих} - U_{вх} - \Delta U_{зс0}$;

– похибку лінійності $\Delta U_{л}$, причому $\Delta U_{л} = \Delta U_{м} - K \cdot U_{вх}$, при чому $K = \frac{y_2 - y_1}{x_2 - x_1}$, де x_1, x_2, y_1, y_2 – координати точок прямої, яка проходить через лінійну ділянку передатної характеристики [6];

Водночас, рівні окремих складових можуть істотно залежати від конкретної схемотехнічної реалізації пристрою. Так, відома схема [4], яку наведено на рис. 1, а, має значну похибку зсуву нуля. Це обумовлено незбалансованістю напруг переходів база-емітер n-p-n і p-n-p транзисторів Т6 і Т7 відповідно.

Для стабілізування напруг колекторних переходів транзисторів вихідних каскадів ядра у схему введено каскоди на транзисторах Т1,Т5 і Т4, Т8 відповідно. Це досить ефективно стабілізує характеристики робочих точок транзисторів Т6 і Т7, зокрема струми колекторів та напруги переходів база-емітер і знижує рівень похибок масштабу і лінійності. Водночас, неідеальність транзисторів Т5 і Т8 каскодів, а саме, залежність β від напруги переходів база-емітер, призводить до зміни їх базових струмів і не дозволяє здійснити подальшу мінімізацію цих складових. Це, у свою чергу, призводить до зміни струмів емітерів транзисторів Т2 і Т3 і, водночас, до зміни напруг база-емітер цих транзисторів, що автоматично передається на вихід схеми і викликає появу похибки зсуву нуля.

Вихідна напруга такої схеми визначається у вигляді:

$$U_{вих} \approx U_{вх} + (U_{бе})_{T2} - (U_{бе})_{T6},$$
$$U_{вих} \approx U_{вх} - (U_{бе})_{T3} + (U_{бе})_{T7},$$

де $U_{вх}$ – вхідна напруга, $(U_{бе})_{T2}, (U_{бе})_{T3}$ – напруга база-емітер транзисторів Т2, Т3, $(U_{бе})_{T6}, (U_{бе})_{T7}$ – напруга база-емітер транзисторів Т6, Т7, причому $(U_{бе})_{T2} \approx (U_{бе})_{T6}, (U_{бе})_{T3} \approx (U_{бе})_{T7}$.

Для інтегральних транзисторів рівень похибки зсуву нуля сягає значень 10÷50 мВ. Похибки масштабу і лінійності істотно залежать від впливу змінення напруг переходів колектор-емітер транзисторів ядра в діапазоні вихідного сигналу. Слід відзначити, що причинами, які негативно впливають на характеристики схеми, є:

1. Залежність напруги перходу база-емітер $U_{бе}$ транзистора від напруги колектор-емітер $U_{ке}$.

2. Залежність колекторного струму $I_к$ транзистора від напруги переходу колектор-емітер, що обумовлено обмеженими значеннями опору колекторного переходу $r_к^*$.

3. Залежність β транзистора від напруги переходу колектор-емітер $U_{ке}$.

Для зменшення похибки зсуву нуля схему запропоновано будувати , як показано на рис. 1, б, тобто уведенням ланцюгів n-p-n і p-n-p транзисторів, які б здійснювали самобалансування напруг p-n переходів. При цьому, вихідна напруга такої схеми визначається:

$$U_{вих} \approx U_{вх} + (U_{бе})_{T2} + (U_{бе})_{T1} - (U_{бе})_{T5} - (U_{бе})_{T6},$$
$$U_{вих} \approx U_{вх} - (U_{бе})_{T3} - (U_{бе})_{T4} + (U_{бе})_{T7} + (U_{бе})_{T8},$$

де $(U_{бе})_{T1} - (U_{бе})_{T8}$ – напруга база-емітер транзисторів Т1-Т8, причому $(U_{бе})_{T1} \approx (U_{бе})_{T5}, (U_{бе})_{T2} \approx (U_{бе})_{T6}, (U_{бе})_{T3} \approx (U_{бе})_{T7}, (U_{бе})_{T4} \approx (U_{бе})_{T8}$.

Така схема має низьку похибку зсуву нуля, яка сягає рівня 200÷500 мкВ, але дещо більшу похибку лінійності, ніж схема на рис. 1, а. Водночас слід зазначити, що залишається проблема залежності напруги переходів база-емітер транзисторів Т5 і Т8 від напруги переходів колектор-емітер.

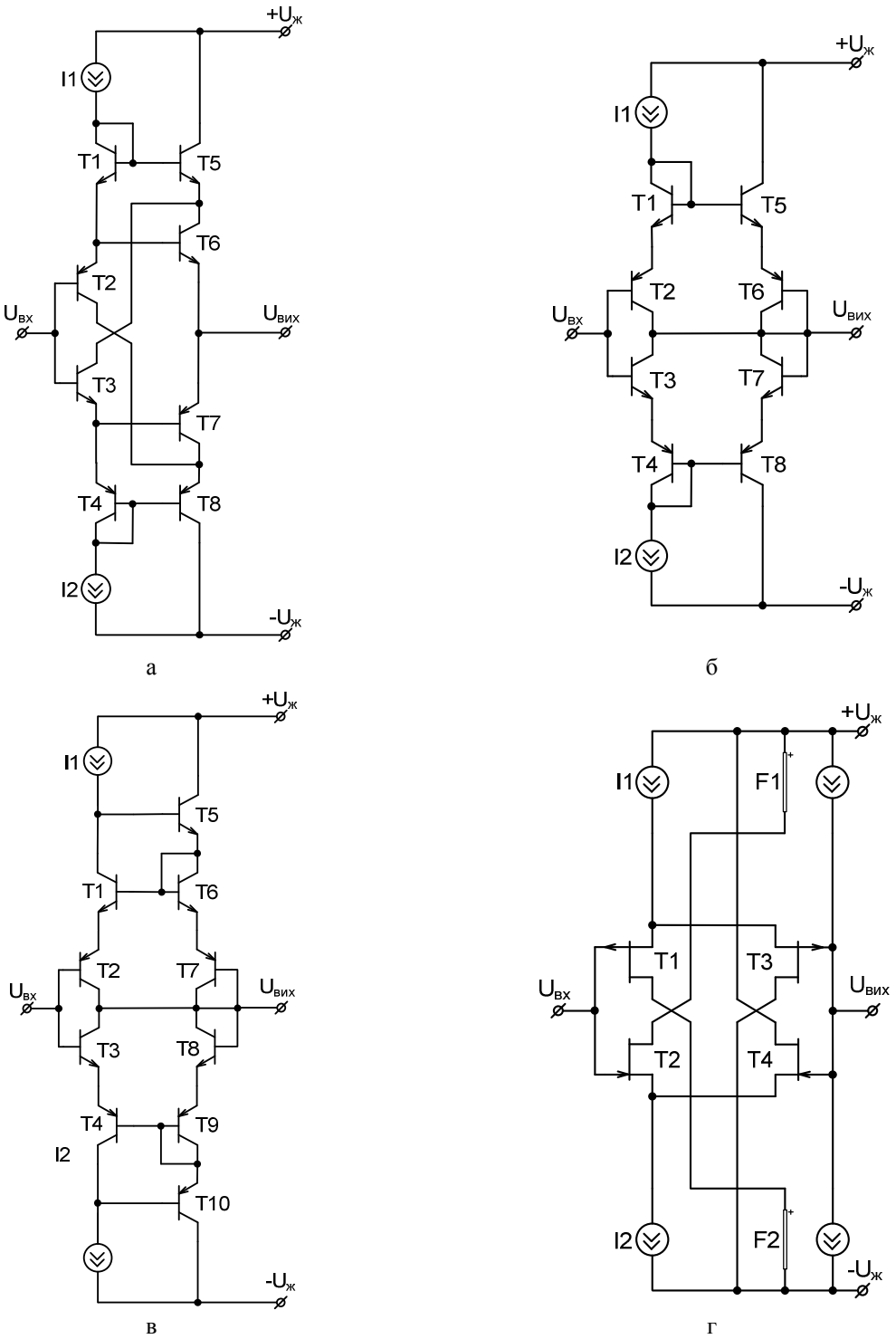


Рисунок 1 – Схемотехнічна організація ядра буферного пристрою: а) без балансування напруг переходів база-емітер; б) із балансуванням напруг переходів база-емітер; в) з каскодуванням струмових виходів на базі схем Уїлсона; г) із диференціальними каскадами на польових транзисторах із самобалансуванням вхід-вихід

Для усунення цих похибок, можна замінити просту каскодну схему на транзисторах Т1,Т5 і Т4, Т8 на каскоди, які побудовано на базі схем Уїлсона. Авторами запропоновано схему буферного пристрою [7], яку зображено на рис. 1, в. Така схема має низьку похибку лінійності, яка прирівнюється до похибки

лінійності схеми на рис. 1, а, та низьку похибку зсуву нуля, на рівні 100÷200 мкВ. Така схемотехнічна організація ядра зменшує вплив напруг переходів база-емітер транзисторів Т6 і Т9, але залишається проблема впливу базового струму транзисторів Т5 і Т10.

Специфікою буферних пристроїв на біполярних транзисторах є принципова наявність вхідного базового струму. Тому кардинальним вирішенням цієї проблеми є використання польових транзисторів з керованими p-n переходами (рис. 1,г). Така схема забезпечує низькі похибку лінійності та похибку зсуву нуля, яка залежить від симетрування напруг стік-витік, а також розкиду напруг заслін-витік пар транзисторів Т1, Т3 і Т2, Т4.

Водночас, треба відзначити, що жодна із розглянутих схем не забезпечує потрібної похибки лінійності в діапазоні вихідного сигналу. Це підтверджено моделюванням похибок масштабу та лінійності ядер буферного пристрою, що наведено на рис. 2.

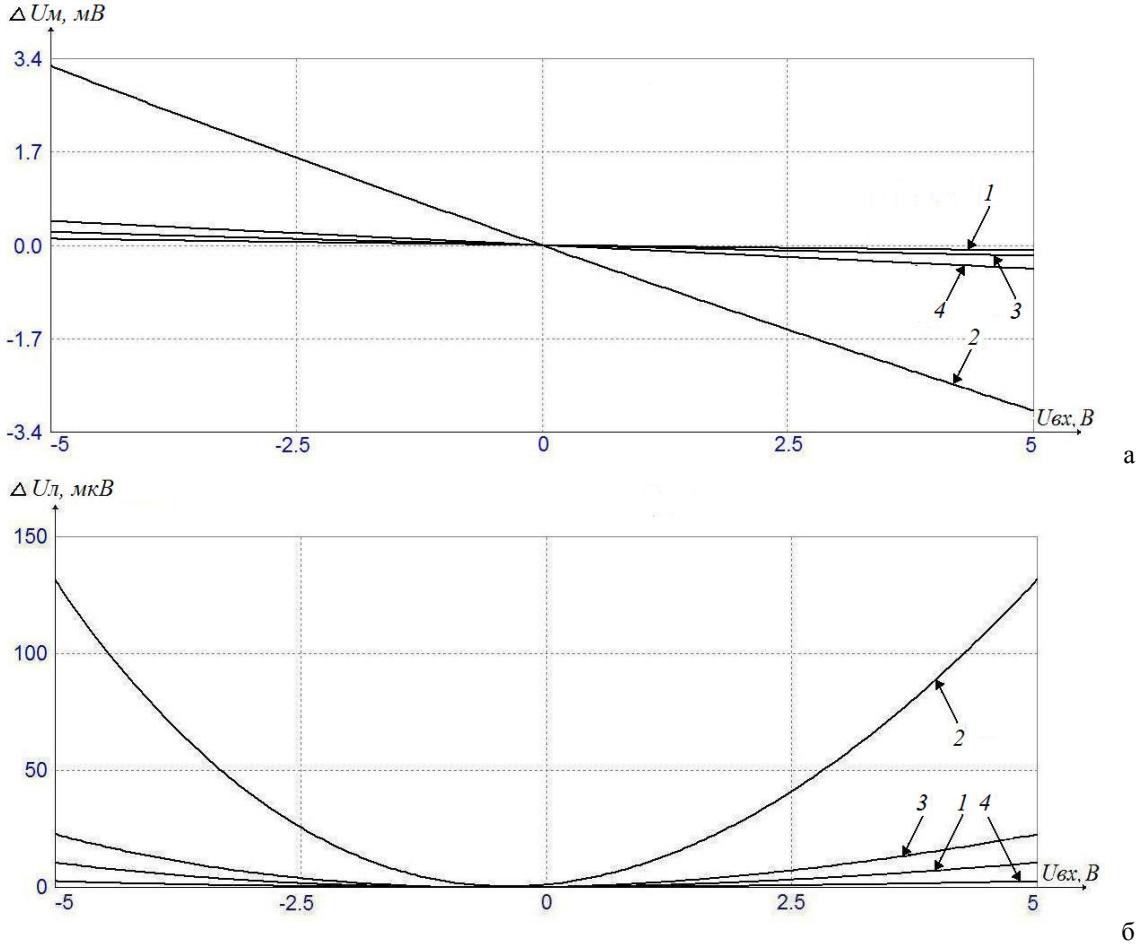
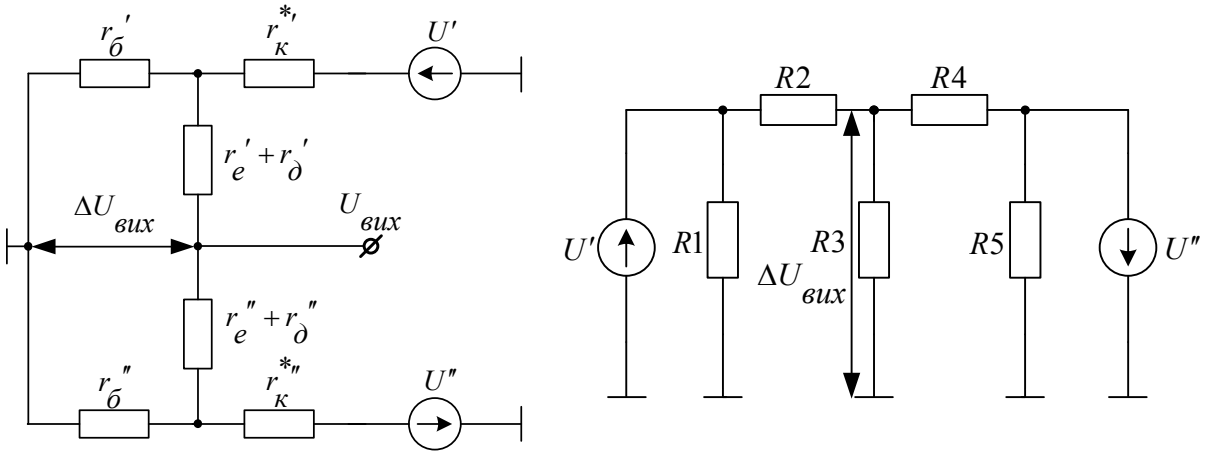


Рисунок 2 – Похибки ядер буферного пристрою: а) масштабу; б) лінійності

На графіках криві 1-4 відносяться до схем ядер буферного пристрою на рис. 1, а-г відповідно. Для визначення складових, які впливають на появу $\Delta U_{вих}$ доцільно розглянути еквіваленту схему заміщення виходу ядра буферного пристрою, яку зображено на рис. 3, а.

Тут: $r_б', r_б''$ – опори баз транзисторів Т5 і Т8 відповідно, $r_к^{*\prime}, r_к^{*\prime\prime}$ – опори колекторів транзисторів Т5 і Т8 відповідно, r_e', r_e'' – опори емітерів транзисторів Т5 і Т8 відповідно, причому $r_e' = r_e'' = r_e$, $r_д', r_д''$ – опори p-n переходів транзисторів Т6 і Т7 у діодному вмиканні відповідно, причому $r_д' = r_д'' = r_д = r_e$, U', U'' – напруги шин додатного і від’ємного живлення відповідно.

Схему доцільно перетворити у такий вигляд, як наведено на рис. 3, б.



а б

Рисунок 3 – Еквівалентні малосигнальні схеми заміщення ядра буферного пристрою:
а) вихідна; б) після перетворення

При цьому:

$$R1 = r_к^{*\prime} + r_б' + \frac{r_к^{*\prime} \cdot r_б'}{2 \cdot r_e}; \qquad R2 = 2 \cdot r_e + r_к^{*\prime} + \frac{2 \cdot r_e \cdot r_к^{*\prime}}{r_б'};$$

$$R3 = \frac{R3' \cdot R3''}{R3' + R3''}, \text{ де } R3' = 2 \cdot r_e + r_б' + \frac{2 \cdot r_e \cdot r_б'}{r_к^{*\prime}}; \qquad R3'' = 2 \cdot r_e + r_б'' + \frac{2 \cdot r_e \cdot r_б''}{r_к^{*\prime\prime}}; \qquad (2)$$

$$R4 = 2 \cdot r_e + r_к^{*\prime\prime} + \frac{2 \cdot r_e \cdot r_к^{*\prime\prime}}{r_б''}; \quad R5 = r_к^{*\prime\prime} + r_б'' + \frac{r_к^{*\prime\prime} \cdot r_б''}{2 \cdot r_e}.$$

Використовуючи метод суперпозиції [8] можемо переписати рівняння (1) у вигляді:

$$\Delta U_{вих} = \Delta U'_{вих} + \Delta U''_{вих}, \qquad (3)$$

де $\Delta U'_{вих} = f(U'), \Delta U''_{вих} = f(U'')$ – прирости напруги по верхньому і нижньому каналах, які у свою чергу визначаються, як:

$$\Delta U'_{вих} = U' \cdot \frac{R3}{R2 + R3};$$
$$\Delta U''_{вих} = U'' \cdot \frac{R3}{R4 + R3}. \qquad (4)$$

Враховуючи вищенаведені залежності та рівняння (3), отримаємо:

$$\Delta U_{вих} = \frac{\left[U' \cdot (R4 + R3) + U'' \cdot (R2 + R3)\right] \cdot R3}{(R2 + R3) \cdot (R4 + R3)}. \qquad (5)$$

Шляхом підстановки в рівняння (5) значень з (2), отримаємо абсолютну похибку. Відносна ж похибка [8] визначається у вигляді:

$$\delta = \frac{\Delta U_{вих}}{U_{вих}} \cdot 100\%.$$

Підставивши у (4) значення з (2) і врахувавши, що в реальних схемах $r_б' \ll r_к^{*\prime}$, $r_б'' \ll r_к^{*\prime\prime}$ і $r_б' \approx r_б''$ отримаємо:

$$\Delta U'_{вих} \approx U' \cdot \frac{2 \cdot r_e}{r_к^{*\prime}}; \quad \Delta U''_{вих} \approx U'' \cdot \frac{2 \cdot r_e}{r_к^{*\prime\prime}}.$$

Легко побачити, що похибка лінійності здебільшого залежить від величини $r_к^{*\prime}$ і $r_к^{*\prime\prime}$, а також r_e, значення якого на 2-3 порядки менше значень $r_к^{*\prime}$ і $r_к^{*\prime\prime}$. Для того, щоб забезпечити побудову прецизійних буферних пристроїв, автори пропонують декілька методів:

1. Уведення до складу ядра каскодів, побудованих на польових транзисторах.
2. Побудова каскодів ядра на складених транзисторах Шиклаї.
3. Використання параметричної стабілізації напруг зміщення транзисторних каскадів ядра.

Перший метод дозволяє підвищити опір виходів по струму [8, 9] (рис. 4, а).

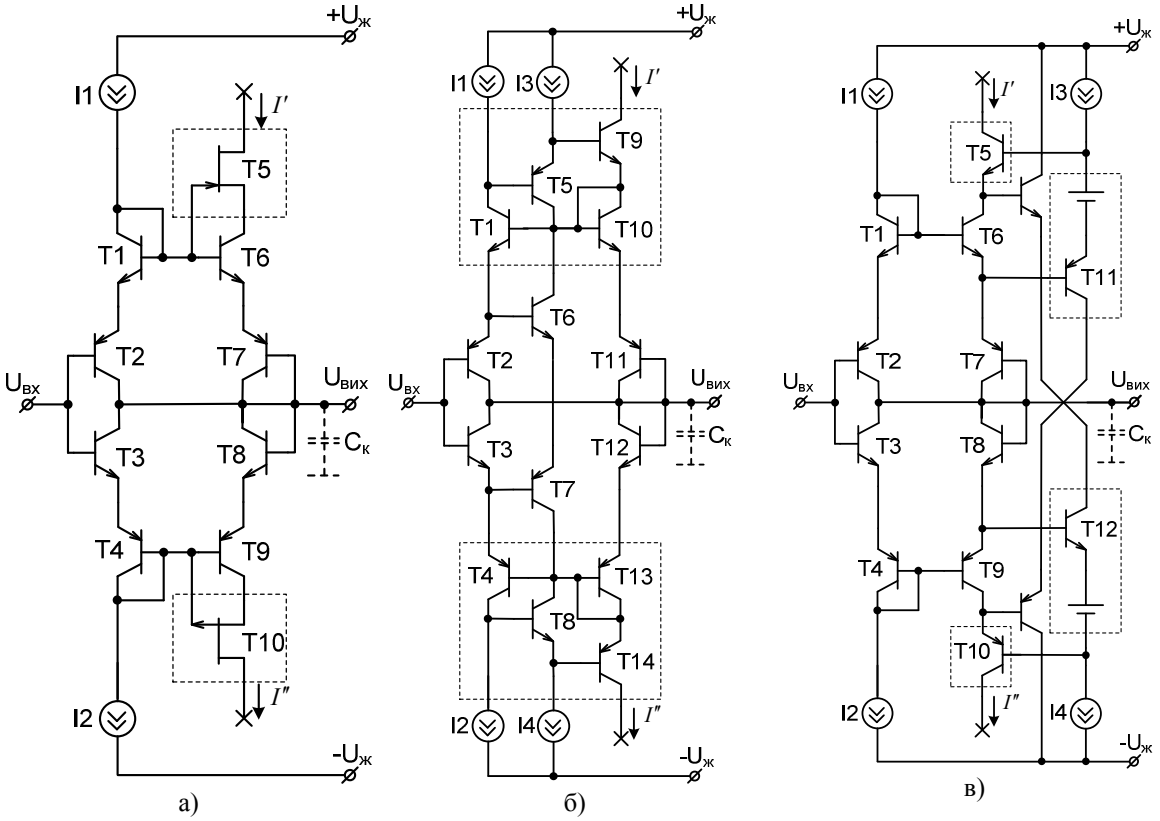


Рисунок 4 – Схемо-функціональна організація вхідних кіл прецизійних буферних пристроїв: а) з каскодами на польових транзисторах; б) з каскодними відбивачами струмів на складених транзисторах ; в) з параметричною стабілізацією напруг колектор-емітер вихідних каскадів

За рахунок цього, забезпечується стабілізація напруг переходів колектор-емітер транзисторів Т6 і Т9, а базовими струмами цих транзисторів можна знехтувати. Враховуючи залежності (4), можемо записати прирости напруги по верхньому і нижньому каналах, як:

$$\Delta U'_{вих} \approx U' \cdot \frac{2 \cdot r_e}{r'_{св}(1 + S' \cdot R'_в)}; \quad \Delta U''_{вих} \approx U'' \cdot \frac{2 \cdot r_e}{r''_{св}(1 + S'' \cdot R''_в)};,$$

де $r'_{св}, r''_{св}$ – диференційні вихідні опори, S', S'' – крутизни передатних характеристик, $R'_в, R''_в$ – об’ємні опори витоків n-канальних і p-канальних польових транзисторів відповідно [9]. Використання каскодів на полових транзисторах дозволяє підвищити лінійність на 1-2 порядки, порівняно з схемою на рис. 1, а.

Другий метод дозволяє зменшити вплив базових струмів транзисторів Т9 і Т14 в β_{n-p-n} і β_{p-n-p} відповідно (рис. 4, б). При цьому похибка лінійності зменшується в $\frac{\beta_{\min}}{2}$ раз, де $\beta_{\min}$ – найменше значення β пари транзисторів Т9 і Т14. Враховуючи залежності (4), можемо записати прирости напруги по верхньому і нижньому каналах, як:

$$\Delta U'_{вих} \approx U' \cdot \frac{4 \cdot r_e}{r'_{вих} \cdot \beta_{n-p-n}}; \quad \Delta U''_{вих} \approx U'' \cdot \frac{4 \cdot r_e}{r''_{вих} \cdot \beta_{p-n-p}}, \qquad (6)$$

Проте необхідно вживати заходів щодо коригування перехідної характеристики, оскільки використання складених транзисторів призводить до появи додаткового полюсу на високих частотах.

Третій метод дозволяє підвищити лінійність із збереженням рівня швидкодії, порівняно зі схемою, яку наведено на рис. 1, а (рис. 4, в). При цьому значення похибки лінійності дещо менше, ніж у схемі із використанням складених транзисторів Шиклаї. Прирости напруги, для такої схеми, описуються співвідношеннями (6).

Графіки похибок масштабу та лінійності, а також перехідних характеристик прецизійних буферних пристроїв наведено на рис. 5 та рис. 6. На графіках криві 1-3 відповідно для схем на рис. 4, а-в. Недоліком розглянутих схем є низька навантажувальна здатність, яка у значній мірі визначається вихідним опором схеми $r_{вих}$.

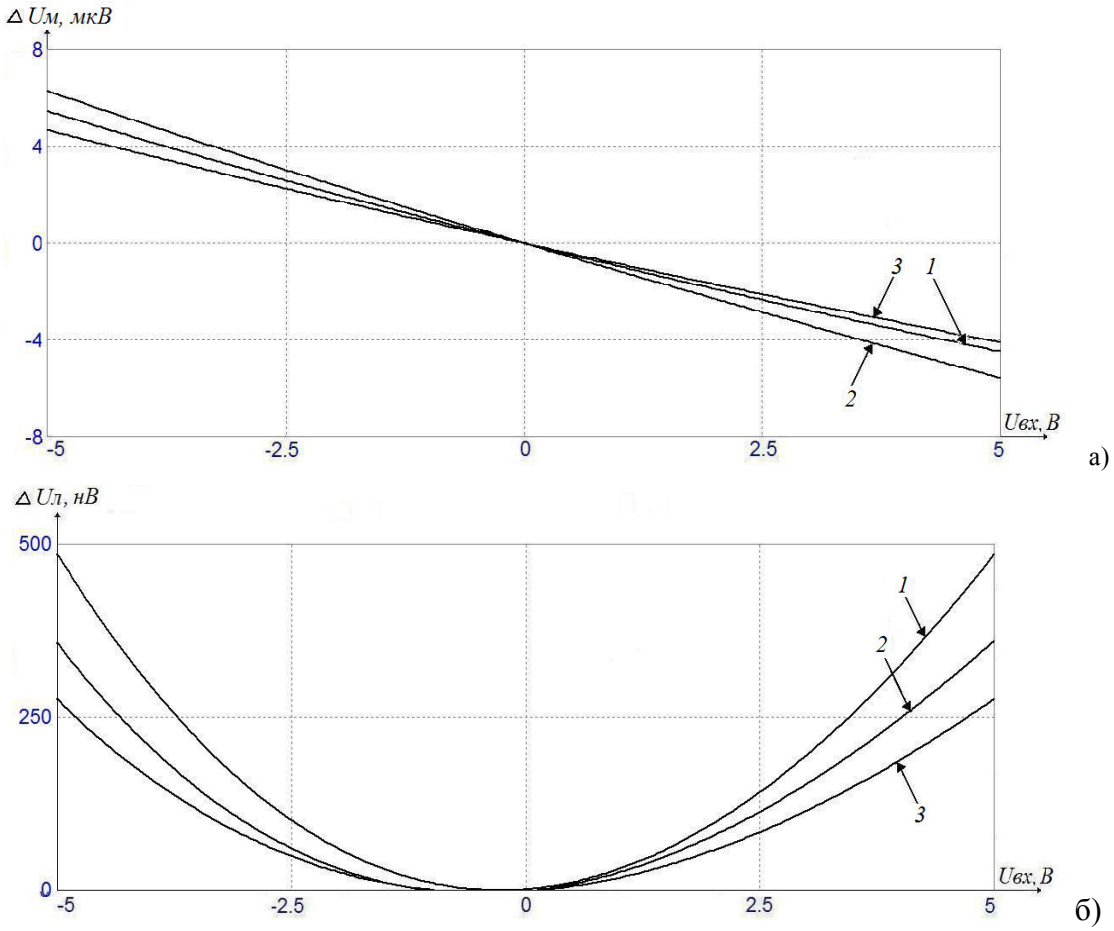


Рисунок 5 – Похибки ядер буферного пристрою з підвищеною лінійністю:
а) масштабу; б) лінійності

При цьому:

$$r_{вих} = r_e,$$

де $r_e = \frac{\varphi_T}{I_e}$, $\varphi_T \approx 25\ мВ$ – термопотенціал, I_e – емітерний струм.

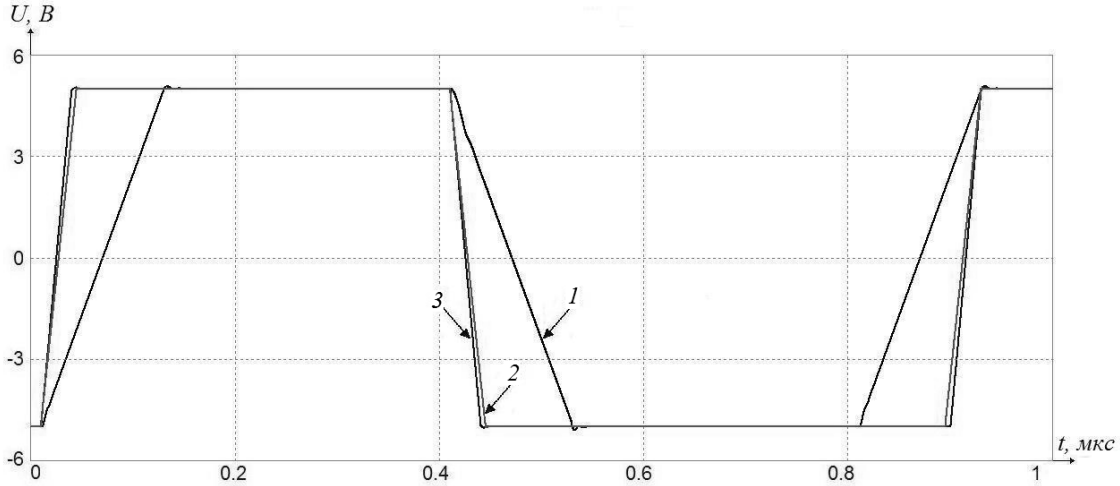


Рисунок 6 – Перехідні характеристики ядер буферного пристрою з підвищеною лінійністю

Ненульове значення вихідного опору призводить до зміни масштабу і погіршення лінійності передатної характеристики. Для підвищення навантажувальної здатності і збереження заданої лінійності, доцільно ввести до схеми двотактний двоканальний підсилювач струму (ДДПС). Узагальнену структуру такого буферного пристрою наведено на рис. 7.

Він складається із підсилювальних каскадів K'_i і K''_i, схеми балансування (СБ) та відбивачів струму ВС1 і ВС2 [10]. СБ дозволяє отримати пропорційну залежність між підсумковими коефіцієнтами передачі і вирівнюванням їх значення і діапазоні сигналу. Умовою самобалансування є виконання рівності: $\frac{I'}{Ip} = \frac{Ip}{I''}$, де Ip – струм робочої точки. При цьому: $K'_i = K''_i$.

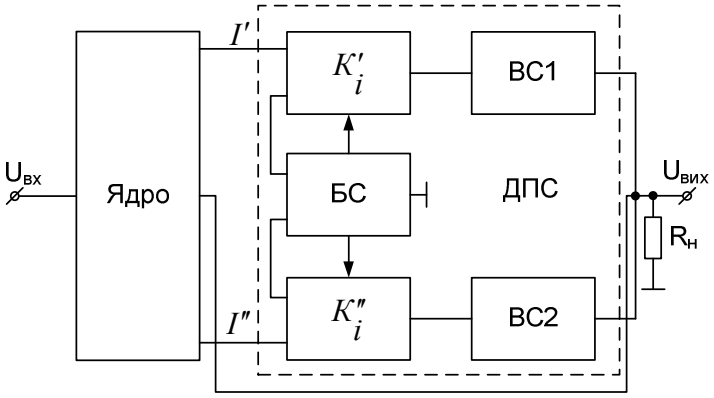


Рисунок 7 – Структурно-функціональна організація прецизійного буферного пристрою на базі двотактної симетричної структури

Введення ДДПС у коло зворотного зв’язку схеми, а саме між ядром і навантаженням, дозволяє зменшити вихідний опір до рівня:

$$r_{вих} = \frac{r_e}{K_i},$$

де K_i – загальний коефіцієнт підсилення ДПС, що визначається, як: $K_i = \frac{2 \cdot K'_i \cdot K''_i}{K'_i + K''_i}$.

Реалізований прецизійний буферний пристрій, побудовано за розглянутою структурно-функціональною організацією на базі двотактної симетричної структури, забезпечує такі характеристики:

- діапазон вхідного сигналу: ± 5В;
- вихідний струм: ± 5 мА;
- похибка зсуву нуля $\Delta U_{зс0} \leq 100$ мкВ;
- похибка масштабу $\delta_{м} = 0.0001\%$;
- похибка лінійності $\delta_{л} = 0.000005\%$.

Висновки

1. Проаналізовано запропоновані методи побудови прецизійних буферних пристроїв на базі двотактних симетричних структур. Показано, що застосування стабілізації напруг переходів колектор-емітер, дозволяє істотно (на 1÷2 порядки) покращити метрологічні характеристики схем.
2. Здійснено порівняльний аналіз статичних похибок передатних характеристик відомих і запропонованих структур двотактних буферних пристроїв. Показано, що запропонований підхід дозволяє значно (на порядок і більше) зменшити похибку зсуву нуля і лінійності при збережені заданого рівня швидкодії.
3. Розглянуто структурно-функціональну організацію прецизійного буферного пристрою з підвищеною навантажувальною здатністю. Доведено, що запропонований підхід дозволяє зменшити вихідний опір на 2÷3 порядки.

Список літератури

1. Walt Kesler. ANALOG-DIGITAL CONVERSION / Walt Kesler – ADI Central Application Department, March 2004. – 1127 p.

2. Alan B. Grebene. Bipolar and MOS analog integrated circuit design / Alan B. Grebene – New Jercy: Whiley Classic Library, 2002. – 915 p.

3. Волович Г.И. Схемотехника аналоговых и аналого-цифровых электрон-ных устройств / Волович Г.И. – М.: Издательский дом «Додэка-XXI», 2005. – 528 с.

4. Бахтиаров Г. Д. Аналого-цифровые преобразователи / Бахтиаров Г. Д., Малинин В. В., Школин В. П.; под. ред. Г. Д. Бахтиарова – М.: Советское радио, 1980. – 280 с., ил.

5. Степаненко И. П. Основы теории транзисторов и транзисторных схем. / Степаненко И. П. – изд. 3-е, перераб. и доп. – М.: «Энергия», 1973. – 608 с., ил.

6. Пат. на корисну модель 51014, Україна, МПК H03K 5/22, G05B 1/00. Буферний каскад / Азаров О. Д., Дудник О. В., Богомолов С. В., Кадук О. В. – № u201000934; Заявлено 29.01.2010; Опубл. 25.06.2010; Бюл. № 12. – 6 с.

7. Азаров О.Д. Похибки лінійності передатної характеристики вхідного каскаду двотактних підсилювачів струму / О.Д. Азаров, С.В. Богомолов, В.Я. Стейскал // Інформаційні технології та комп'ютерна інженерія. Вінницький національний технічний університет – 2010. – №3(19). – С. 4-12.

8. Касаткин А.С. Электротехника: [учеб. пособие для вузов] /А.С. Касаткин, М.В. Немцов– изд. 4-е, перераб. – М.:Энергоатомиздат, 1983. – 440 с., ил.

9. Титце У. Полупроводниковая схемотехника: [справочное руководство] / У. Титце, К. Шенк; [пер. с нем.] –М.: 1982. – 512 с., ил.

10. Азаров О.Д. Двотактні підсилювачі постійного струму для багаторозрядних перетворювачів форми інформації, що самокалібруються : монографія / О. Д. Азаров, В. А. Гарнага. – Вінниця: ВНТУ, 2011. – 156 с.

Відомості про авторів

Азаров Олексій Дмитрович – завідувач кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 58-02-25.

Богомолов Сергій Віталійович – аспірант кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. +38-097-131-83-78, e-mail: bogomolovsergiy@rambler.ru.

УДК 681.325.5

О.Д. АЗАРОВ, О.І. ЧЕРНЯК

Вінницький національний технічний університет, Вінниця

СТРУКТУРНА ОРГАНІЗАЦІЯ ПОБІТОВОГО ДОДАВАННЯ І ВІДНІМАННЯ КОДІВ ЗОЛОТОЇ 1-ПРОПОРЦІЇ ІЗ ВРАХУВАННЯМ ЗНАКІВ

Анотація. Описані структурна організація та робота пристрою конвеєрного побітового додавання і віднімання довільних форм прямих кодів золотої 1-пропорції із врахуванням їх знаків. Пристрій має зменшені витрати обладнання.
Ключові слова: код золотої пропорції, побітове віднімання, побітове додавання, послідовний код.
Аннотация. Описаны структурная организация и работа устройства конвейерного побитового сложения и вычитания произвольных форм прямых кодов золотой 1-пропорции с учетом их знаков. Устройство имеет уменьшенные затраты оборудования.
Ключевые слова: код золотой пропорции, побитовое вычитание, побитовое сложение, последовательный код.
Abstract. The structural organization and operating of bit-serial pipe-line adding and subtraction device for golden 1-ratio ones complement codes in any forms with signs are described. The device have less hardware.
Keywords: code golden ratio, bitwise subtraction, bitwise addition, the serial code.

Актуальність

Коди золотої 1-пропорції забезпечують побітове виконання усіх арифметичних операцій з найменшою довжиною перенесення, що дозволяє зменшити витрати обладнання при побудові пристроїв. При побітовій обробці найчастіше виконуються додавання і віднімання над кодами зі знаками. Тому актуальною є розробка структурної організації побітового додавання і віднімання кодів золотої 1-пропорції із врахуванням знаків.

Аналіз останніх досліджень

Алгоритмічні основи побітової обробки кодів золотої 1-пропорції описано у [1]. Пристрій побітового додавання кодів золотої 1-пропорції описано у [2], а у [3] – пристрій побітового віднімання цих кодів. Дані пристрої призначені для побітового додавання і віднімання додатних кодів. Як описано у [4], побітове виконання арифметичних операцій починаючи зі старших розрядів повинно виконуватись над прямими послідовними кодами зі знаками. При такій обробці знак послідовного коду розташований одразу після старшої одиниці, що досягається шляхом обміну місцями знаку і старшої одиниці.

Постановка задач

Метою статті є опис результатів, отриманих у процесі розробки пристрою побітового додавання і віднімання прямих кодів золотої 1-пропорції. На вхід пристрою поступають послідовні коди золотої 1-пропорції зі знаками. Пристрій повинен визначати, видаляти з кодів і запам’ятовувати знаки операндів. Необхідно також розташувати у потрібному місці старші одиниці операндів. В залежності від знаків операндів і сигналу операції, пристрій повинен встановлювати істину операцію: додавання або віднімання. Крім того, пристрій повинен формувати прямий код результату і вставляти в нього знак після старшої одиниці. Таким чином, при розробці пристрою побітового додавання і віднімання кодів золотої 1-пропорції із врахуванням знаків постає задача розробки побітового пристрою, що виконує такі функції:

визначення, видалення з кодів і запам’ятовування знаків операндів;

встановлення істинної операції;

виконання побітового додавання або віднімання кодів золотої 1-пропорції;

формування коду результату зі знаком;

Пристрій побітового додавання і віднімання із врахуванням знаків

Побітове додавання і віднімання кодів золотої 1-пропорції із врахуванням знаків має певні особливості. На входи пристрою, починаючи зі старших розрядів, надходять послідовні коди операндів X та Y, а на виході, починаючи зі старших розрядів, формується послідовний код результату Z. При цьому на кожному такті використовується код проміжного результату S_i, що являє собою частину розрядів, через які можливе розповсюдження перенесення у наступному такті виконання операції. Для врахування знаку проміжного коду використовується сигнал Зх, одиничне значення якого вказує, що знак проміжного результату співпадає із знаком операнду X.

Обробка знаків операндів починається з надходження старших одиниць на кожному з входів X та Y. Наступними надходять знаки операндів, які разом із сигналом операції використовуються для встановлення операції і запам’ятовуються. Сигнал операції разом з черговими розрядами операндів Xi, Yi та сигналом Зх формують чергову суму розрядів, що може мати значення 0, -1, 1 або 2. Чергова сума розрядів додається до попереднього проміжного результату Si-1 та формує попереднє значення чергового проміжного результату, над яким виконується повна згортка. При цьому формується черговий проміжний результат Si та значення розряду результату zi, як логічне АБО старшого розряду Si-1 та перенесення від згортки. Це значення затримується на один такт. У випадку побітового віднімання для запобігання обнуління проміжного результату додатково виконується розгортка отриманого на попередньому такті

значення розряду результату zi-1 у старші розряди Si. При надходженні знаку лише одного операнду до надходження знаку другого операнду примусово встановлюється операція віднімання. Це призводить до розгортки чергового розряду результату і запобігає обнуліню проміжного результату. Розгортка забороняється протягом чотирьох тактів після надходження сигналу початку чергового коду операнду. З урахуванням розгортки формується остаточне значення чергового розряду результату Zi.

Структурна організація пристрою побітового додавання і віднімання із врахуванням знаків подана на рис. 1. Пристрій має вхід Оп управління операцією; входи x та y, на які поступають чергові розряди операндів; вхід С тактування, вхід СЧ сигналу початку числа; вхід ПВ початкового встановлення та вихід z чергового розряду результату. Крім того, пристрій містить блок аналізу знаків (БАЗ) для аналізу, запам'ятовування та видалення знаків операндів; блок стробування (БС) для вироблення сигналів скидання тригерів та заборони розгортки; блок операції (БО) для вироблення сигналу операції; блок обробки розрядів (БОР) для виконання операції над черговими розрядами операндів та блок формування сигналів (БФС) для формування проміжного коду та сигналу Зх.

Також даний пристрій містить регістр Рг1 для зберігання двох молодших розрядів проміжного коду; регістр Рг2 для зберігання трьох старших розрядів даного коду і попереднього значення чергового розряду результату; тригер для зберігання ознаки Зх (ТЗх); блок розгортки (БР) для розгортки старшого розряду результату коду та блок формування результату (БФР) для вставляння знаку у код результату.

Пристрій працює у такий спосіб. Перед початком роботи на пристрій подається нульовий сигнал ПВ, що поступає на БС. БС формує нульовий сигнал скидання R, що поступає на R-входи всіх тригерів і скидає їх у нульовий стан. Тактові імпульси поступають на вхід С пристрою, а з нього на тактові входи всіх тригерів. На входи x та y пристрою поступають коди операндів, а на вхід Оп поступає сигнал операції (0 – додавання, 1 – віднімання). Чергові розряди операндів із входів x та y пристрою поступають на входи iX та iY БАЗ. БАЗ видаляє знаки з кодів операндів, запам'ятовує їх та виробляє одиничне чи нульове значення сигналу примусової розгортки Р. Якщо першим надходить знак Х, то БАЗ видає нульовий сигнал $\overline{Sx}$, який встановлює ТЗх, в одиничний стан. Це означає, що на даний момент знак проміжного результату S_i дорівнює знаку операнду Х. Після видалення і аналізу знаків операндів на кожному такті пристрій реалізує операції додавання або віднімання у два етапи. Для цього використовується ознака Зх. На першому етапі в залежності від операції, ознаки Зх та знаків операндів виконується віднімання або додавання їх чергових розрядів. Результатом такої операції може бути -1, 0, 1 чи 2. На другому етапі цей результат в залежності від його знаку віднімається або додається до проміжного коду. Перший етап операції виконує блок обробки розрядів. На кожному такті з виходів oX та oY БАЗ чергові розряди операндів поступають на входи X та Y БОР.З виходів Zx та Zy БАЗ знаки операндів поступають на входи Zx та Zy БО, на вхід Оп якого поступає сигнал операції. БО встановлює необхідну операцію. Сигнал операції з виходу БО поступає на входи Оп БОР та БР. БОР в залежності від операції, ознаки Зх та значень чергових розрядів операндів формує результат обробки розрядів: 0, -1, 1 чи 2. Слід відзначити, що ознака Зх враховується лише при відніманні і впливає на знак одиничного результату. Результат обробки розрядів з БОР поступає на БФС. Крім того, на БФС поступає з Рг1 і Рг2 попередній проміжний код, а з ТЗх – ознака Зх. БФС формує новий проміжний код, ознаку Зх та попереднє значення чергового розряду результату. Черговий проміжний код та попереднє значення чергового розряду результату поступають на регістри Рг1 і Рг2 для запам'ятовування і використання на наступному такті. Чергова ознака Зх поступає для запам'ятовування на тригер ТЗх. На наступному такті два старші розряди проміжного коду та попереднє значення чергового розряду результату поступають на входи БР, на інші входи якого поступають сигнал операції Оп та сигнал дозволу розгортки Р. Якщо встановлена операція віднімання і дозволена розгортка, то при виконанні умови БР розгортає одиничне попереднє значення розряду результату у старші розряди проміжного коду. З виходів БР старші розряди чергового проміжного коду поступають на відповідні входи БФС. Крім того, на виході БР формується черговий розряд результату, що поступає на вхід Z БФР. На інші входи БФР поступають ознака Зх та знаки операндів. БФР вставляє знак перед старшою одиницею коду результату. Після обробки останніх розрядів операндів на вході пристрою протягом чотирьох тактів встановлюється нульове значення сигналу СЧ, що поступає на вхід БС. БС формує сигнал скидання R усіх тригерів крім тригерів Рг2, в яких знаходяться старші розряди чергового проміжного коду. Протягом наступних чотирьох тактів ці розряди"виштовхуються" з Рг2. Крім того, БС протягом чотирьох тактів формує нульове значення сигналу Р, що блокує розгортку попереднього значення чергового розряду результату. Блок формування сигналів БФС формує черговий проміжний код, попереднє значення чергового розряду результату та ознаку Зх. На рис. 2 представлені часові діаграми роботи пристрою побітового додавання і віднімання із врахуванням знаків, отримані шляхом моделювання у середовищі Active HDL. Діаграми підтверджують правильність роботи пристрою. Пристрій містить 196 логічних елементів з базового набору І, АБО, НЕ, І-НЕ, АБО-НЕ.

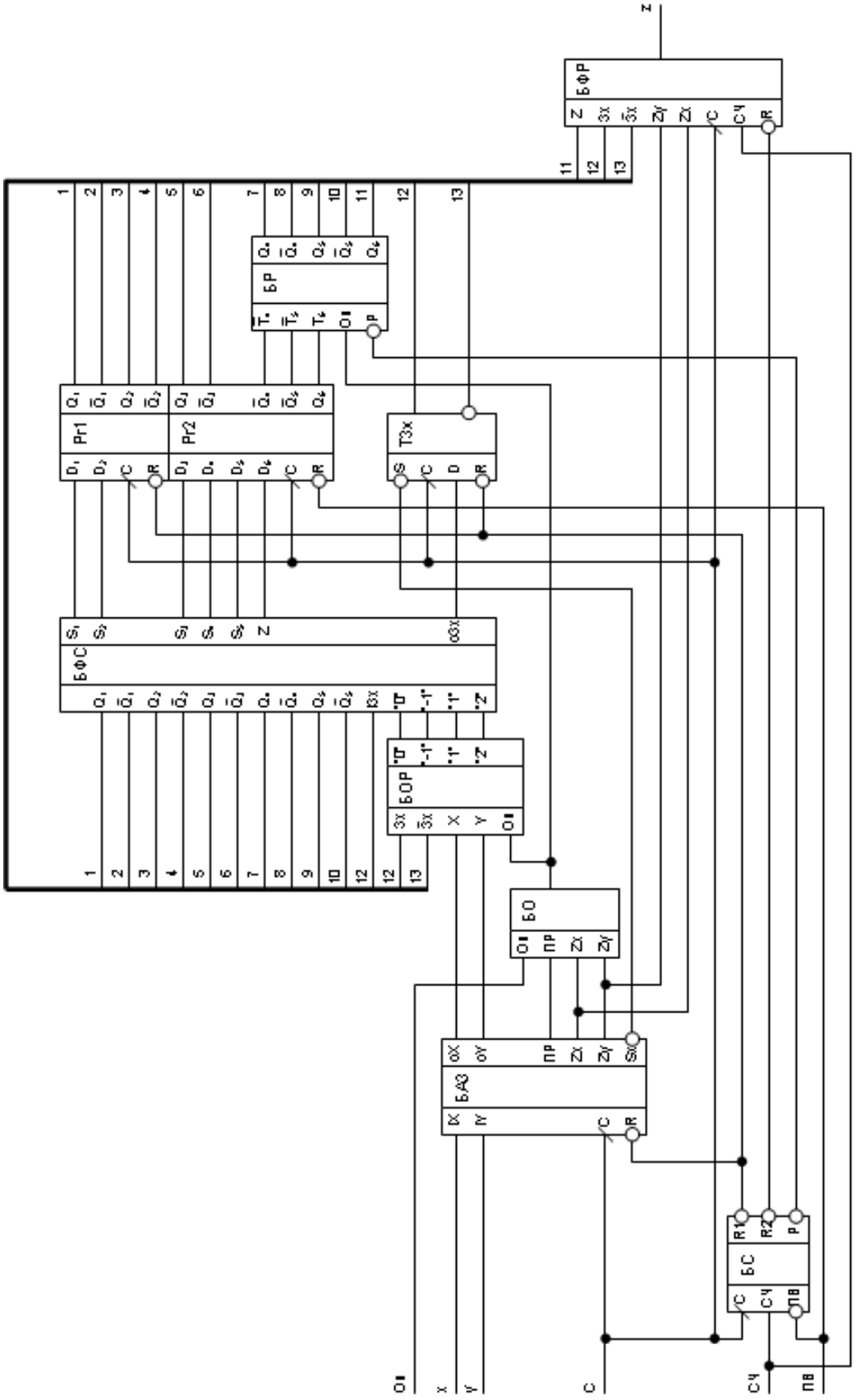


Рисунок 1 – Структурна організація пристрою побітового додавання і віднімання із врахуванням знаків

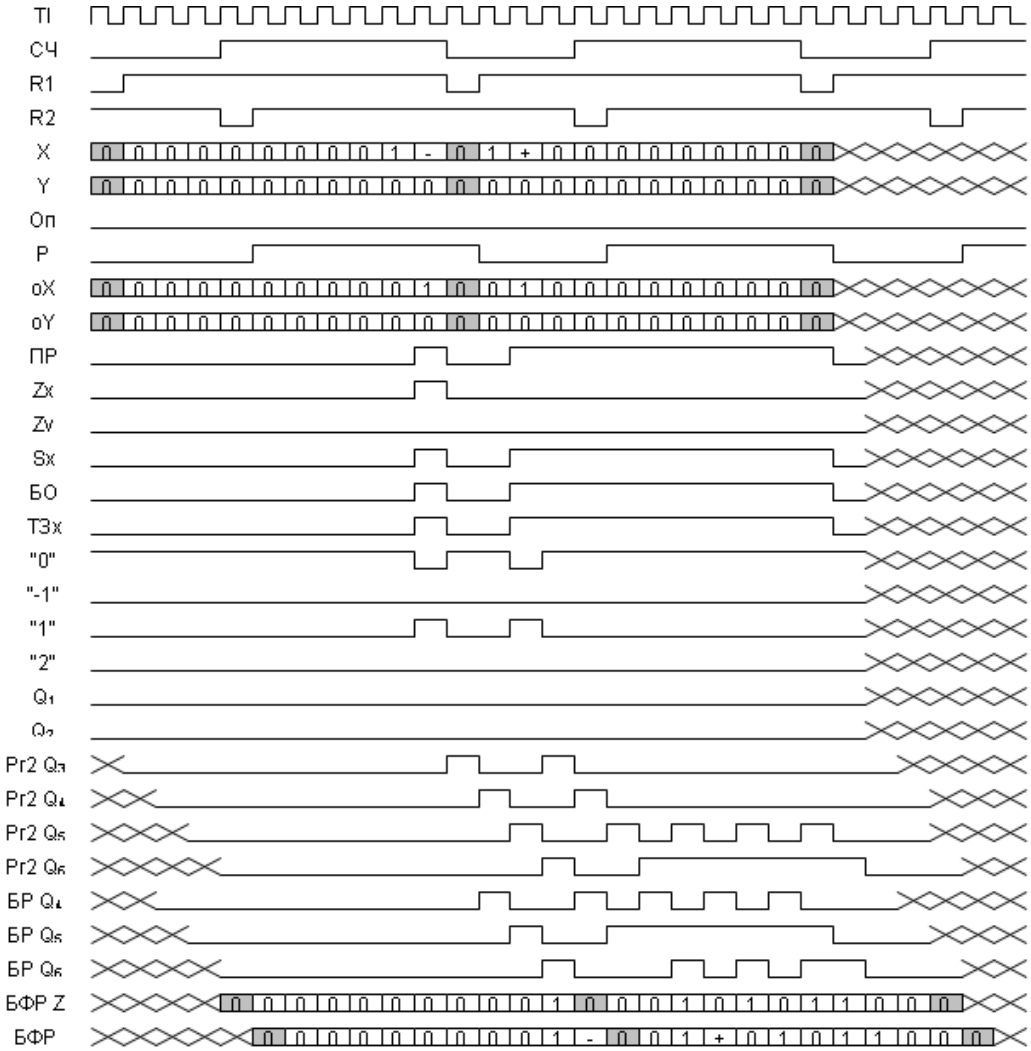


Рисунок 2 – Часові діаграми роботи пристрою побітового додавання і віднімання із врахуванням знаків

Висновки

1. Вперше розроблена структурна організація пристрою побітового додавання і віднімання прямих послідовних кодів золотої пропорції із врахуванням знаків.

2. Розроблена схема промодельована у середовищі Active HDL. Результати моделювання підтвердили працездатність пристрою.

Список літератури

1. Алгоритми побітової обробки кодів золотої пропорції / Азаров О. Д., Черняк О. І. // Інформаційні технології та комп'ютерна інженерія. – Вінниця : ВНТУ. – 2006. –№2(6). С. 28–43.

2. Схемотехнічні основи побітового додавання кодів золотої пропорції / Азаров О. Д., Черняк О. І. // Інформаційні технології та комп'ютерна інженерія. – Вінниця : ВНТУ. – 2007. – №1. – С. 9-17.

3. Схемотехнічні основи побітового віднімання кодів золотої пропорції / Азаров О. Д., Черняк О. І. // Вісник ВПІ. – Вінниця : ВНТУ. – 2008. – №2. – С. 56-60.

4. Азаров А. Д., Черняк А. И. Полнофункциональная побитовая обработка результатов аналого-цифрового преобразования // Тези доповідей Третьої Міжнародної науково-практичної конференції "Методи та засоби кодування, захисту й ущільнення інформації", Вінниця, 20-22 квітня 2011р. С.208-209.

Відомості про авторів

Азаров Олексій Дмитрович – завідувач кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 58-02-25.

Черняк Олександр Іванович – старший викладач кафдри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

УДК 004.728.4(045)

І.А. ЖУКОВ, Ю.Ю. ІСКРЕНКО

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПЕРЕДАЧІ БІТОВОГО ПОТОКУ ШУМОПОДІБНИМИ СИГНАЛАМИ ІЗ ЗАДАНОЮ СИНХРОНІЗАЦІЄЮ

Анотація. Впровадження і використання в роботі аеропортів широкосмугового бездротового зв'язку при управлінні повітряним рухом транспортних засобів забезпечує підвищення пропускної спроможності і дальності дії під час інтенсивно працюючих операцій з такими даними як навігація та контроль.

Ключові слова: передача мультимедійного трафіка, широкосмуговий бездротовий зв'язок, шумоподібні сигнали, синхронізація трафіка.

Аннотация. Внедрение и использование в работе аэропортов широкополосной беспроводной связи при управлении воздушным движением транспортных средств, обеспечивает повышение пропускной способности и дальности действия во время интенсивно работающих операций с такими данными как навигация и контроль.

Ключевые слова: передача мультимедийного трафика, широкополосная беспроводная связь, шумоподобные сигналы, синхронизация трафика.

Annotation. Introduction and use in-process of air-ports by broadband wireless networks to control air traffic, provides the increase of bandwidth and distance of action during intensive workings operations with such information as a navigation and control.

Key words: multimedia traffic transmission, broadband wireless network, noise-shaped signals, traffic synchronization.

Вступ

За рахунок великої швидкості передачі інформації, великого радіусу і дальності дії цей підхід здатний зменшити час координації і відгуку повітряних транспортних засобів. Передаючи інформацію шумоподібними сигналами підвищується завадостійкість, тим самим зменшується час затримки передачі інформації під час польоту.

Найбільш перспективним засобом колегіального управління комп'ютерними системами і територіально розподіленими мобільними об'єктами в реальному часі є впровадження бездротових технологій *WiFi* і *WiMAX* [1]. Перша технологія забезпечує передачу бітового потоку в невеликому радіусі, з максимальною швидкістю передачі 2 Мбіт/с. Для цифрової широкосмугової інтеграції більше підходить друга технологія з радіусом дії до 100 км і швидкістю передачі рівної 50 Мбіт/с [2].

В основу технології *WiIMAX* покладена стільникова топологія передачі інформації, де кожна базова станція (БС) соти повинна забезпечувати у рамках соти передачу мультимедійного трафіку (ММТ) із заданою якістю обслуговування *QoS*.

Актуальність

Однією з особливостей процесу функціонування мережі є управління під час виникнення різних конфліктних ситуацій. До конфліктних ситуацій можна віднести найбільш поширені: перевантаження мережі в цілому, що характерно для передачі ММТ в реальному часі; перевантаження її окремих компонентів або сегментів. У запропонованому методі синхронізації при виникненні перевантаження під час роботи мережі виконується розподіл пам'яті і каналів на пріоритетні та не пріоритетні потоки.

Мета

Для колегіального управління в сотах потрібна взаємодія технології *WiMAX*, високонадійних і завадостійких способів передачі між базовими і абонентськими станціями (АС).

Постановка задач

1) Оптимізувати пам'ять і канали в комутаційному вузлі певного типу. Синхронізація мультимедійного трафіку;

2) Коригувати мультимедійний трафік в умовах появи перешкод, за рахунок розширення спектру і використання шумоподібних сигналів (ШПС).

Розв’язання задач

Синхронізація мультимедійного трафіку при передачі комутаційним вузлом

Відомі два основні компоненти мультимедійного трафіку – аудіо компонент, який повинен передаватися без великих затримок і відео компонент, затримки можливі, але мають бути мінімальні. При використанні цих технологій в процесі колегіального управління повітряним рухом виникає проблема недостатньої пропускної спроможності і дальності дії існуючих систем управління. Для безпечного і ефективного управління повітряним рухом потрібна точна і своєчасна обробка інформації картографічного інтерфейсу на аеродромі, картографічного інтерфейсу смуги посадки, зони очікування; в умовах картографічних траєкторій, що постійно накладаються. Це представлення є вузловим місцем колегіального управління, оскільки і диспетчер, і штурман бачать хто, де, і як здійснює повітряний рух. Результатом виконання є система що підтримує управління великою кількістю об'єктів в більшій зоні дії.

Втрати одного потоку визначаються числом каналів, їх продуктивністю і пам'яттю.

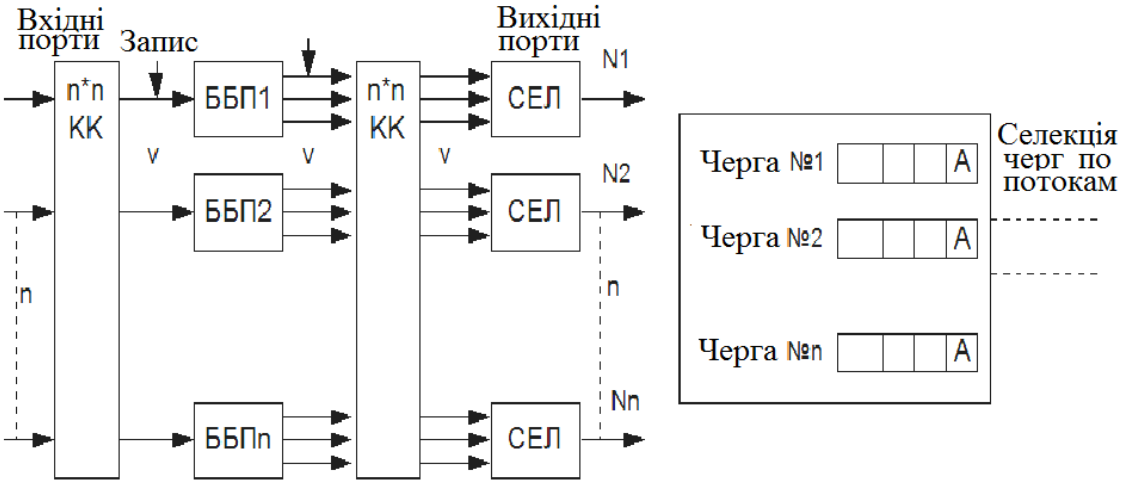


Рисунок 1 – Структурна схема комунікаційного вузла з мультибуферною пам'яттю і системою синхронізації мультимедійного трафіку.

Послідовність розрахунку втрат при передачі ММТ із заданою інтенсивністю виглядає таким чином:

1) функціональна структура вузла комутації;
2) часова діаграма передачі;
3) граф переходу з одного стану в інший;
4) система рівнянь.

Для реалізації такого підходу пропоновані вузли з інтенсивностями поступання інформації - λ_1, λ_2 і загальна пам'ять.

У функціональній структурі для синхро передач необхідно вказати для кожного синхронізованого потоку число каналів і елементів пам'яті окремо. Для побудови графіку переходів необхідно побудувати тимчасову діаграму переходів. При цьому має бути визначена функціональна структура синхронної передачі ММТ для пріоритетного потоку λ_1, числом пам'яті, що не перевищує задану затримку. Для другого непріоритетного потоку, можна збільшити в два рази пам'ять, оскільки затримки не впливають на потік, але в результаті втрат буде менше. Якщо співвідношення λ_1 і λ_2 один до одного, то число каналів може бути однакове, якщо інтенсивність вступу λ_2 в два рази більше, отже, ресурс буде задіяний в два рази більше, тому що відношення λ_1 до λ_2 – 0,5. Це співвідношення використовується, тому що на вході має бути синхроно передаючий потік, який за кількістю компонент, що приймаються, поступається пріоритетному.

Процес синхронізації може бути реалізований у рамках комунікаційного вузла, що складається з блоків мультибуферної пам'яті і набору кросточечних комутаторів (рис. 1) [3]. Після проходження інформаційного потоку через мультибуферну частину вузла інформація поступає в систему синхронізації мультимедійного трафіку, де відбувається її подальший розподіл на пріоритетні і не пріоритетні потоки. Збільшення пам'яті дає можливість не втратити ці пакети, оскільки при зайнятих каналах, пам'ять також зайнята, як наслідок йдуть втрати. Пам'ять зберігається, а продуктивність підвищується за рахунок числа каналів і пропускної спроможності кожного каналу, чим швидше вони працюють, тим менше втрат.

Один з потоків передачі ММТ є пріоритетним і не повинен мати втрат більше допустимого рівня, другий потік - непріоритетний і не повинен мати великих затримок при передачі [4, 5].

У цифровому зв'язку на кожні п'ять посилок контейнерів відео доводиться один аудіо контейнер, для правильної синхронізації необхідно серед інтенсивності вступу відео контейнерів уклинювати аудіо контейнери, виконуючи цю умову тимчасова діаграма вступу складатиметься з двох інтенсивностей (λ_1 - відео і λ_2 - аудіо). λ_1 відео - втрати мають бути у рамках допустимого значення, λ_2 - має свої вимоги - аудіо трафік не повинен мати великих затримок, вони не мають бути більше допустимих.

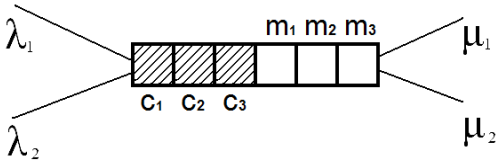


Рисунок 2 – Структура комутатора з трьома каналами передачі і трьома елементами пам'яті.

Запропонований комутаційний вузол в який поступають компоненти ММТ: λ_1 і λ_2, в цьому вузлі є пам'ять і є декілька каналів, для цього вузла формується тимчасова діаграма. Одна вісь – час, друга – стани (рис. 3).

При формуванні цієї діаграми головним є обчислення виштовхування непріоритетних компонент у втрати (*G*), тобто оптимізація роботи системи.

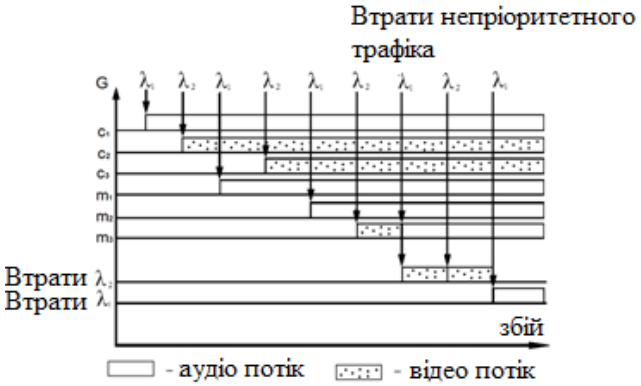


Рисунок 3 – Часова діаграма переходів станів

Послідовно відбувається процес використання усіх каналів і усіх елементів пам'яті до моменту виникнення втрат. Часова діаграма дозволяє отримати граф переходів станів розподілу пам'яті і каналів.

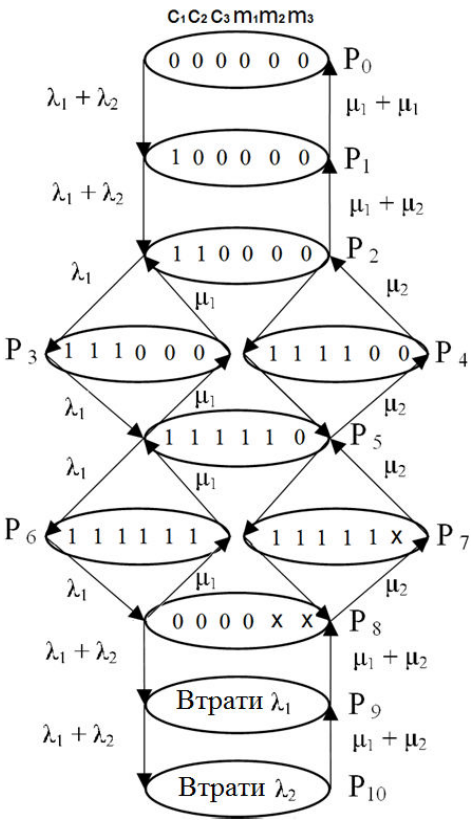


Рисунок 4 – Граф переходу з одного стану в інший.

На основі графа переходів будується система рівнянь, за результатами рішення якої вибирається оптимальне значення. Що дозволяє скласти втрати і отримати коефіцієнт втрат, скласти коефіцієнти передачі і отримати коефіцієнт ефективної передачі без втрат.

$$\begin{cases} -P_0(\lambda_1+\lambda_2)+P_1(\mu_1+\mu_2)=0 \\ P_0(\lambda_1+\lambda_2)+P_2(\mu_1+\mu_2)-P_1(\lambda_1+\lambda_2)-P_1(\mu_1+\mu_2)=0 \\ P_1(\lambda_1+\lambda_2)-P_2(\mu_1+\mu_2)-\lambda_1P_2+\mu_1P_3-\lambda_2P_2+\mu_2P_4=0 \\ \lambda_1P_2-\mu_1P_3-\lambda_1P_3+\mu_1P_5=0 \\ \lambda_2P_2-\lambda_2P_4+\mu_2P_5-\mu_2P_4=0 \\ \lambda_1P_3-\mu_1P_5+\lambda_2P_4-\mu_2P_5-\lambda_1P_5+\mu_1P_6-\lambda_2P_5+\mu_2P_7=0 \\ \lambda_1P_5-\mu_1P_6-\lambda_1P_6+\mu_1P_8=0 \\ \lambda_2P_5-\mu_2P_7-\lambda_2P_7+\mu_2P_8=0 \\ \lambda_1P_6-\mu_1P_8+\lambda_2P_7-\mu_2P_8-P_8(\lambda_1+\lambda_2)+P_9(\mu_1+\mu_2)=0 \\ P_8(\lambda_1+\lambda_2)-P_9(\mu_1+\mu_2)-P_9(\lambda_1+\lambda_2)+P_{10}(\mu_1+\mu_2)=0 \\ P_9(\lambda_1+\lambda_2)-P_{10}(\mu_1+\mu_2)=0 \end{cases}$$

Для знаходження значень матриці великої розмірності, вона була розбита на дві частини.

При постійних: λ_2, μ_1, μ_2.

При λ_2= 0,2, μ_1= 0,5, μ_2= 1; $n_1 = \lambda_1$, $n_2 = \lambda_2$, $m_1 = \mu_1$, $m_2 = \mu_2$.

Second system n1 :=0,1 n_2 :=0,1 m_1 :=0,1 m_2 :=0,1; K := $n_1 + n_2 + m_1 + m_2$.

Інтенсивності вступу інформації відомі та змінюються для знаходження оптимального значення та опису побудови матриці, складеної на основі системи рівнянь (1). Розрахунки виконуються системою комп'ютерної алгебри *MathCad*:

Замінюючи значення одного рівняння системи рівнянь на одиницю відбувається обчислення і розрахунок результатів :

$A2 := stack(A21, A22)\ \ rank(A2) = 11;$

$P2 := lsolve\ (A2, B2).$

$$A21:=\begin{bmatrix} -(n1+n2) & m1+m2 & 0 & 0 & 0 & 0 & 0 & 0 \\ n1+n2 & -K & m1+m2 & 0 & 0 & 0 & 0 & 0 \\ 0 & n1+n2 & -K & m1 & m2 & 0 & 0 & 0 \\ 0 & 0 & n1 & -(n1+m1) & 0 & m1 & 0 & 0 \\ 0 & 0 & n2 & 0 & -(n2+m2) & m2 & 0 & 0 \\ 0 & 0 & 0 & n1 & n2 & -K & m1 & m2 \end{bmatrix}$$

$$A22:=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & n1 & -(n1+m1) & 0 & m1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & n2 & 0 & -(n2+m2) & m2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & n1+n2 & -K & m1+m2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & n1+n2 & -(m1+m2) \end{bmatrix}$$

Після обчислень отримуємо наступний результат кожного стану запропонованої системи:
$P2_0$ = 0,795; $P2_1$ = 0,159; $P2_2$ = 0,032; $P2_3$ = 0,06358; $P2_4$ = 0,0636; $P2_5$ = 0,01272; $P2_6$ = 0,002543; $P2_7$ = 0,00255; $P2_8$ = 0,0005086; $P2_9$ = 0,0001017; $P2_{10}$ = 0,00002034;

Наступним кроком є побудова графіку залежності λ_1 від P, при різних значеннях λ_1 вибирається одне значення *P*, наприклад при λ_1= 0,1, 0,2, 0,3, 0,4, 0,5, 0,6, 0,7, 0,8, 0,9, 1.

Приклад розрахунку одного зі значень при λ_1= 0,2 представимо у вигляді:
$P2_0$ = 0,721; $P2_1$ = 0,192; $P2_2$ = 0,051; $P2_3$ = 0,017; $P2_4$ = 0,012; $P2_5$ = 0,03896; $P2_6$ = 0,01324; $P2_7$ = 0,00896; $P2_8$ = 0,002961; $P2_9$ = 0,0007895; $P2_{10}$ = 0,0002105;

Міняючи одну з інтенсивностей передачі або інтенсивність вступу, можна зробити висновок про значення μ і λ. При μ = 1 (незадовільне), λ = 2 (буде дуже багато втрат), якщо навпаки, то результат покращується. Підставляючи *P*5, при різних значеннях, будується графік:

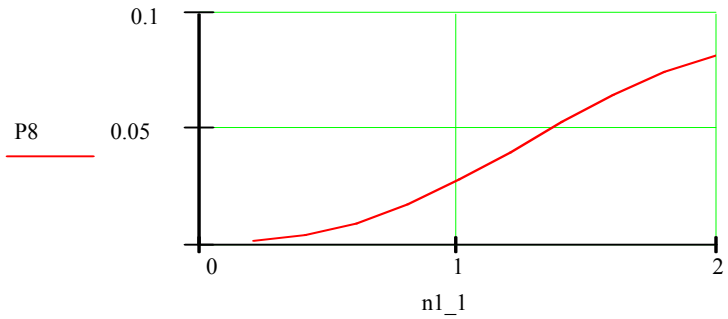


Рисунок 5 – Графік залежності втрат пріоритетного і не пріоритетного трафів.

Формування пакету передачі бітового потоку по радіоспектру

Стандарт 802.16 на фізичному рівні використовує технологію *Orthogonal Freuency Division Multiplexing* (*OFDM*).

У специфікації для вказівки різної тривалості по осі часу використовується поняття тимчасової одиниці *TS* = 1/(15000x2048) с. Передача радіоканалом здійснюється кадрами завдовжки *Tf* = 307200x*TS* = 10 мс. При цьому підтримуються дві структури кадрів. Одна - для випадку частотного дуплексу (*Frequency Division Duplex*, *FDD*), інша - для часового дуплексу (*Time Division Duplex*, *TDD*) [6, 7].

Структура кадрів. Спочатку розглядається кадр для випадку *FDD*. Кожен кадр (рис. 6) складається з 20 слотів завдовжки *Tslot* = 0.5 мс, які пронумеровані від 0 до 19. Окрім цього, виділяється поняття підкадру, який складається з двох сусідніх слотів, тобто підкадр з номером і включає слоти з номерами 2*i* і 2*i*+1.

У разі *FDD* низхідний (*downlink*) і вхідний (*uplink*) канали передаються на різних частотах, тому в кожному 10 мс інтервалі часу є 10 підкадрів для "завантаження" і 10 підкадрів для "вигрузки".

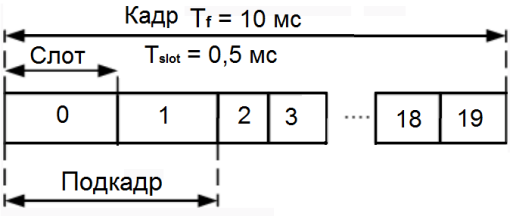


Рисунок 6 – Структура кадру при *FDD* передачі.

Розглянемо кадр для випадку *TDD*. При тимчасовому дублексуванні каналів кадр ділиться на низхідний і вихідний субкадри (їх співвідношення може гнучко змінюватися в процесі роботи, залежно від необхідної смуги пропускання для низхідних і вихідних каналів). Розділені спеціальним інтервалом (рис. 7). У низхідному каналі інформація від базової станції передається у вигляді послідовності пакетів [2]. Дані про параметри пакету, його довжину, момент початку передачі, а також про його приналежність до певного з'єднання містяться в карті низхідного каналу *DL - MAP*. Цей випадок представлено на рис. 7 [2]:

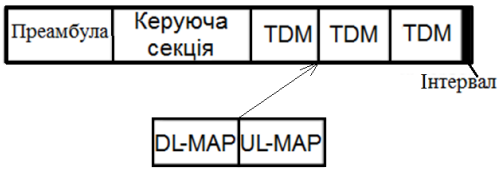


Рисунок 7 – Структура кадру при *TDD* передачі.

Після розгляду формування кадрів технології *WIMAX,* можливе застосування шумоподібних сигналів чисельними послідовностями Баркера для їх передачі. Для цього необхідно, щоб бітовий потік мав службову інформацію. Бітовий потік повинен передаватися невеликими посилками (кадрами) за допомогою перешкод кодових чисельних послідовностей Баркера. Знаючи розмір передаваного кадру, можна розрахувати ширину смуги частот по Баркеру.

Існують наступні чисельні послідовності Баркера, приведені в таблиці [8]:

Спектр кодової послідовності. Амплітудний спектр $|H(x)|$ кодової послідовності знаходиться безпосередньо з виразу [8]:

$$|H(\omega)| = \sqrt{\sum_{n=1}^{N}\sum_{k=1}^{N} a_n a_k \cos(n-k)\omega\tau_0} .$$

Таблиця. Кодові послідовності Баркера.

№	A_n при n													R_{2l}
	1	2	3	4	5	6	7	8	9	10	11	12	13	
3	1	1	-1	-	-	-	-	-	-	-	-	-	-	-1/3
4	1	1	-1	1	-	-	-	-	-	-	-	-	-	+1/4
5	1	1	1	-1	1	-	-	-	-	-	-	-	-	1/5
7	1	1	1	-1	-1	1	-1	-	-	-	-	-	-	-1/7
11	1	1	1	-1	-1	-1	1	-1	-1	1	-1	-	-	-1/11
13	1	1	1	1	1	-1	-1	1	1	-1	1	1	1	1/13

Енергетичний спектр кодової послідовності Баркера $R(\mu)= 1/N$ описується виразом:

$$|H(x)|^2 = N(1-\frac{1}{N}+\frac{1}{N}\frac{\sin N x}{x}) .$$

При $R(\mu) = -1/N$

$$|H(x)|^2 = N(1+\frac{1}{N}-\frac{1}{N}\frac{\sin N x}{x}) .$$

Інформація передається передавачами таким чином, що байт розкладається та передається і в цей же потік вступають перешкоди, при отриманні сигнали перетворюються і фільтруються приймачами.

Висновки

Обґрунтовані вимоги передачі мультимедійного трафіку потоком пакетів при використанні технології *WIMAX*, які визначають оптимальне значення λ_1 і λ_2, а також оптимальне значення пам'яті і рівень продуктивності, необхідний для надійної передачі.

Розрахована точність синхронізації ММТ для певної швидкості передачі (λ_1 - пріоритетний, λ_2 - непріоритетний, пам'ять - певне значення) і смуги пропускання. Смуга залежатиме від того з якою інтенсивністю передається інформація шумоподібними сигналами.

Розглянуто рішення завдань, пов'язаних зі знаходженням оптимального розподілу ресурсів пам'яті і каналів на комутаційному вузлі запропонованого типу [3], в якому можна передавати стійкий ШПС.

Список літератури

1. Вишневский В.М., Ляхов А.И. Портной С.Л., Шахнович И.В. Широполосные беспроводные сети передачи информации. – М.: Техносфера, 2005. – 592 с.

2. Вишневский В. Энциклопедия WIMAX. Путь к 4G. – М.: Техносфера, 2009. – 470 с.

3. Ластовченко М.М., Ярошенко В.Н., Биляк В.И. Математические аспекты проектирования интеллектуальных коммутационных систем передачи ММТ // Математ. машины и системы. – 2001. – № 6. – С. 56-69.

4. Радченко Ю.С., Радченко Т.А. Эффективность кодового разделения сигналов с неизвестным временем прихода // Труды междунар. конф. Радиолокация, навигация, связь. – 1999. – С. 507-514.

5. Баскадов С. И. Радиотехнические цепи и сигналы. – М.: Высш. шк., 2000. – 462 с.

6. Скляр Б. Цифрвая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.

7. Ратынский М.В. Основы сотовой связи. – М.: Радио и связь, 1998. – 248 с.

8. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

Відомості про авторів

Жуков Ігор Анатолійович – завідувач кафедри комп'ютерних систем та мереж, Національний Авіаційний університет, пр. Комарова 1, м. Київ, 03058, тел. (044)-406-76-78.

Іскренко Юрій Юрійович – аспірант кафедри комп'ютерних систем та мереж, Національний Авіаційний університет, пр. Комарова 1, м. Київ, 03058, тел. -099-051-37-49, e-mail: iskra2008@gmail.com.

УДК 621.375.024

С. М. ЗАХАРЧЕНКО, О. В. БОЙКО, Г. С. ЗАХАРЧЕНКО

Вінницький національний технічний університет, Вінниця

АНАЛІЗ СТАТИЧНИХ ПОХИБОК ЦИКЛІЧНОГО АЦП ІЗ ВАГОВОЮ НАДЛИШКОВІСТЮ

Анотація. Розглянуто структуру циклічного АЦП, досліджено процес утворення і накопичення статичних похибок функціональними блоками, що входять до складу даного АЦП та приведено математичні співвідношення для їх визначення. Проведено класифікацію статичних похибок, що дозволяє віднести їх до адитивних або мультиплікативних і показано вплив даних складових на передатну характеристику. Доведено, що розриви кодувальної характеристики, спричинені накопиченням похибок і відхиленням основи системи числення, можна уникнути застосувавши вагову надлишковість.

Ключові слова: похибки циклічного АЦП, циклічний АЦП, алгоритмічний АЦП, вагова надлишковість, статичні похибки АЦП.

Аннотация. Рассмотрено структуру циклического АЦП, исследован процесс образования и накопления статических погрешностей функциональными блоками, входящих в состав данного АЦП и приведены математические соотношения для их определения. Проведена классификация статических погрешностей, что позволяет отнести их к аддитивным или мультипликативным, и показано влияние данных составляющих на передаточную характеристику. Доказано, что разрывы кодирующей характеристики, вызванные накоплением погрешностей и отклонением основания системы счисления, можно избежать применив весовую избыточность.

Ключові слова: погрешности циклического АЦП, циклическое АЦП, алгоритмический АЦП, весовая избыточность, статические погрешности АЦП.

Annotation. The structure of cyclic ADC is observed, investigated the formation and accumulation of static errors of cyclic ADC functional blocks and given mathematical relations for their determination. The classification of static errors has been carried out, it’s allow include this error to the additive or multiplicative, and shows how data elements in the transfer characteristic. It is proved that breaks coding characteristics caused by the accumulation of errors and deviation calculation system, can be avoided by applying weight redundancy.

Keywords: error cyclic ADC, cyclic ADC, algorithmic ADC, weight redundancy, static error of the ADC.

Вступ

Одним із видів АЦП послідовного наближення є алгоритмічні (циклічні) АЦП, які виділяються середньо швидкодією і роздільною здатністю до 14 біт. Широко використовується даний тип АЦП для побудови конвеєрних АЦП, а також як калібруючий АЦП, тому виробники перетворювачів форм інформації приділяють велику увагу данному сектору ринка АЦП. Циклічні АЦП вирізняються простою структурою, низькою потужністю споживання і малими фізичними розмірами на кристалі. Крім того, дані АЦП є розрядно-незалежними, тобто збільшення розрядної сітки перетворювача не веде за собою збільшення або ускладнення апаратного забезпечення.

Хоча алгоритмічні АЦП мають низку переваг, але їх точність значно залежить від точності виконання кожним блоком, що входить до АЦП, своїх функцій, тому що похибки накопичуються і циркулюють від циклу до циклу. Отже залишкові напруги зсуву на операційних підсилювачах і конденсаторах, шум і інжекція заряду через МОН-ключі, а також точність коефіцієнта множення є дуже критичними факторами.

Мета

Аналіз запропонованих методів структурно-функціональної організації прецизійних ПСН та ПНН на базі ДПС, їх передатних характеристик та похибок лінійності.

Задачі дослідження

Для досягнення мети необхідно розв’язати такі задачі:

- розглянути структуру циклічних АЦП;
- побудувати модель, що описує функціонування циклічного АЦП;
- дослідити процес утворення і накопичення статичних похибок циклічного АЦП.

Структура циклічного АЦП

Блок-схема алгоритмічного АЦП представлена на рис.1

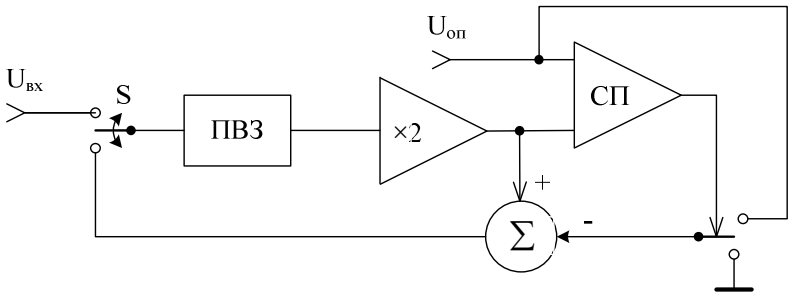


Рисунок 1 – Циклічний АЦП

Робота циклічного АЦП базується на алгоритмі МакЧарльза [1]. Під час першого циклу перетворення вхідний сигнал U_{BX} проходить через пристрій вибірки-зберігання, множиться на 2 і порівнюється з

опорною напругою $U_{ОП}$. Якщо $2 \cdot U_{ВХ} \geq U_{ОП}$, то старший біт встановлюється в "1", а $U_{ОП}$ віднімається від подвоєної вхідної напруги і отримане значення передається на наступний цикл. У тому випадку, коли $2 \cdot U_{ВХ} < 0$, то старший біт встановлюється в "0", а значення подвоєної вхідної напруги передається на наступний цикл. Аналогічним чином визначаються й інші розряди вихідного коду. Тобто для n-розрядного АЦП на кожному циклі алгоритму напругу можна представити за допомогою послідовності співвідношень:

$$
\begin{aligned}
&1)\, U_0 = 2 \cdot U_{вх};\\
&2)\, U_1 = 2 \cdot U_0 - a_0 \cdot U_{оп} \Rightarrow 2 \cdot 2U_{вх} - a_0 \cdot U_{оп} \Rightarrow 4U_{вх} - a_0 \cdot U_{оп};\\
&3)\, U_2 = 2 \cdot U_1 - a_1 \cdot U_{оп} \Rightarrow 2 \cdot (2U_0 - a_0 \cdot U_{оп}) - a_1 \cdot U_{оп} \Rightarrow 8U_{вх} - 2a_0 U_{оп} - a_1 U_{оп};\\
&4)\, U_3 = 2 \cdot U_2 - a_2 \cdot U_{оп} \Rightarrow 2 \cdot (2U_1 - a_1 \cdot U_{оп}) - a_2 \cdot U_{оп} \Rightarrow 16U_{вх} - 4a_0 U_{оп} - 2a_1 U_{оп} - a_2 U_{оп};\\
&5)\, U_4 = 2 \cdot U_3 - a_3 \cdot U_{оп} \Rightarrow 2 \cdot (2U_2 - a_2 \cdot U_{оп}) - a_3 \cdot U_{оп} \Rightarrow 32U_{вх} - 8a_0 U_{оп} - 4a_1 U_{оп} - 2a_2 U_{оп} - a_3 U_{оп};\\
&\qquad\qquad ...\\
&i)\, U_{i+1} = 2 \cdot U_i - a_i \cdot U_{оп} \Rightarrow 2 \cdot (2U_{i-1} - a_{i-1} \cdot U_{оп}) - a_i \cdot U_{оп} \Rightarrow\\
&\qquad\qquad \Rightarrow 2^{i+2} \cdot U_{вх} - 2^i \cdot a_0 U_{оп} - 2^{i-1} \cdot a_1 U_{оп} - 2^{i-2} \cdot a_2 U_{оп} - ... - a_i U_{оп}.
\end{aligned}
\tag{1}
$$

В загальному випадку напругу, що формується за допомогою алгоритму МакЧарльза на i-тому кроці можна представити за допомогою співвідношення:

$$U_{i+1} = 2 \cdot U_i + a_i \cdot U_{оп}, \tag{2}$$

де $a_i \in \{0,1\}$ – двійкове значення i-го розряду вихідного коду.

Проте рівність (1) описує ідеальний процес перетворення двійкового циклічного АЦП. Реальне значення напруги можна представити за допомогою співвідношення: $U_i' = U_i + \Delta U_i$, де U_i – ідеальне значення напруги на i-тому циклі перетворення, ΔU_i – відхилення напруги на i-тому циклі перетворення, тому для n-розрядного АЦП реальне значення напруги на кожному циклі перетворення визначається наступними рівностями:

$$
\begin{aligned}
&1)\, U_0 = 2 \cdot (U_{вх} + \Delta U_{вх});\\
&2)\, U_1 = 2 \cdot (U_0 + \Delta U_0) - a_0 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 2 \cdot 2(U_{вх} + \Delta U_{вх}) - a_0 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 4(U_{вх} + \Delta U_{вх}) - a_0 \cdot (U_{оп} + \Delta U_{оп});\\
&3)\, U_2 = 2 \cdot (U_1 + \Delta U_1) - a_1 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 2 \cdot (2(U_0 + \Delta U_0) - a_0 \cdot (U_{оп} + \Delta U_{оп})) - a_1 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow\\
&\qquad \Rightarrow 8(U_{вх} + \Delta U_{вх}) - 2a_0 (U_{оп} + \Delta U_{оп}) - a_1 (U_{оп} + \Delta U_{оп});\\
&4)\, U_3 = 2 \cdot (U_2 + \Delta U_2) - a_2 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 2 \cdot (2(U_1 + \Delta U_1) - a_1 \cdot (U_{оп} + \Delta U_{оп})) - a_2 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow\\
&\qquad \Rightarrow 16(U_{вх} + \Delta U_{вх}) - 4a_0 (U_{оп} + \Delta U_{оп}) - 2a_1 (U_{оп} + \Delta U_{оп}) - a_2 (U_{оп} + \Delta U_{оп});\\
&5)\, U_4 = 2 \cdot (U_3 + \Delta U_3) - a_3 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 2 \cdot (2(U_2 + \Delta U_2) - a_2 \cdot (U_{оп} + \Delta U_{оп})) - a_3 \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow\\
&\qquad \Rightarrow 32(U_{вх} + \Delta U_{вх}) - 8a_0 (U_{оп} + \Delta U_{оп}) - 4a_1 (U_{оп} + \Delta U_{оп}) - 2a_2 (U_{оп} + \Delta U_{оп}) - a_3 (U_{оп} + \Delta U_{оп});\\
&\qquad\qquad ...\\
&i)\, U_{i+1} = 2 \cdot (U_i + \Delta U_i) - a_i \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow 2 \cdot (2(U_{i-1} + \Delta U_{i-1}) - a_{i-1} \cdot (U_{оп} + \Delta U_{оп})) - a_i \cdot (U_{оп} + \Delta U_{оп}) \Rightarrow\\
&\qquad \Rightarrow 2^{i+2} \cdot (U_{вх} + \Delta U_{вх}) - 2^i \cdot a_0 (U_{оп} + \Delta U_{оп}) - 2^{i-1} \cdot a_1 (U_{оп} + \Delta U_{оп}) - 2^{i-2} \cdot a_2 (U_{оп} + \Delta U_{оп}) - ... - a_i (U_{оп} + \Delta U_{оп}).
\end{aligned}
\tag{3}
$$

Кожен блок, що входить до даного перетворювача (пристрій вибірки-зберігання, схема підсилення (множення) сигналу на основу системи числення, схема віднімання і компаратор) вносить свою похибку у вихідний код.

Моделювання роботи циклічного АЦП

Основним принципом функціонування циклічного АЦП є послідовне визначення ваг розрядів шляхом підсилення вхідного сигналу і віднімання від нього опорної напруги. Для моделювання роботи перетворювача використано базові схеми реалізації пристрою вибірки-зберігання, схем підсилення і віднімання. Кожна із схем, що входить до даної моделі, вносить похибку у результуючий сигнал, тому розглянемо дані блоки і визначимо за якими законами вони працюють.

Пристрій вибірки-зберігання (рис. 2):

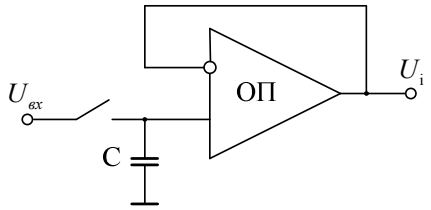


Рисунок 2 – Пристрій вибірки-зберігання

Даний блок слугує для фіксації значення аналогового сигналу в певний момент часу. Закон функціонування ідеального пристрою вибірки-зберігання:

$$U_i = U_{вх} \ . \tag{4}$$

Схема підсилення (множення) сигналу на коефіцієнт α (основу системи числення) (рис. 3):

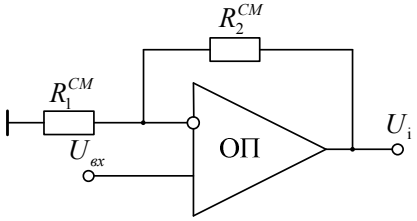


Рисунок 3 – Схема підсилення сигналу на α

$$U_i = U_{вх} \cdot (1 + \frac{R_2^{CM}}{R_1^{CM}}) . \tag{5}$$

Виходячи із співвідношення (5) систему числення перетворювача можна визначити за формулою:

$$\alpha = 1 + \frac{R_2^{CM}}{R_1^{CM}} = 1 + k^{CM} \ . \tag{6}$$

Відповідно з урахування виразу (6) співвідношення (5) можна представити у вигляді

$$U_i = U_{вх} \cdot \alpha \ . \tag{7}$$

Схема віднімання (рис. 4):

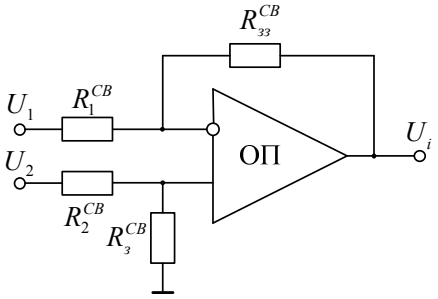


Рисунок 4 – Схема віднімання

$$U_i = U_2 \cdot (\frac{(R_{зз}^{CB} + R_1^{CB}) \cdot R_з^{CB}}{(R_з^{CB} + R_2^{CB}) \cdot R_1^{CB}}) - U_1 \cdot (\frac{R_{зз}^{CB}}{R_1^{CB}}) . \tag{8}$$

Якщо представити $\frac{(R_{зз}^{CB} + R_1^{CB}) \cdot R_з^{CB}}{(R_з^{CB} + R_2^{CB}) \cdot R_1^{CB}}$ як k_1^{CB} та $\frac{R_{зз}^{CB}}{R_1^{CB}}$ як k_2^{CB} то вираз (8) можна представити наступним чином:

$$U_i = k_1^{CB} \cdot U_2 - k_2^{CB} \cdot U_1 . \tag{9}$$

Оскільки $R_1^{CB} = R_2^{CB} = R_з^{CB} = R_{зз}^{CB}$ то $k_1^{CB} = k_2^{CB} = 1$ і вираз (8) матиме вигляд: $U_i = U_2 - U_1$.

Таким чином з урахуванням вище отриманих співвідношень роботи блоків і відповідно до розглянутого алгоритму аналогово-цифрового перетворення напруга на виході схеми віднімання, що передається на наступний цикл в процесі перетворення описується виразом:

$$U_{(i+1)} = U_i \cdot (1 + k^{CM}) - U_{оп} . \tag{10}$$

Аналіз статичних похибок циклічного АЦП

Похибка перетворення циклічного АЦП визначається передусім відхиленням аналогових елементів перетворювача від номіналу і накопиченням даних похибок від циклу до циклу як мультиплікативних і адитивних.

Відносну похибку ваги і-го розряду може бути знайдено за формулою

$$\delta U_i = \Delta U_i / U_i, \tag{11}$$

$$\Delta U_i = U_i' - U_i, \tag{12}$$

де ΔU_i - абсолютна похибка сигналу на *i*-тому циклі перетворення; U'_i – реально отримане значення сигналу на *i*-тому циклі перетворення; U_i – значення сигналу на *i*-тому циклі ідеального процесу перетворення.

Похибка формування сигналу на виході пристрою вибірки-зберігання обумовлена похибкою задання тактових інтервалів в процесі перетворення; проходженням керуючого сигналу через паразитні ємності ключових елементів.

Основними характеристиками точності конденсаторів є допуск на номінальну ємність при виготовленні, температурний коефіцієнт ємності (ТКЄ), опір витоку діелектрика, коефіцієнт абсорбції.

При наявності відхилення ємності від свого номіналу її реальне значення визначається як:

$$C_{зб} = C_{зб} \cdot (1+\delta C_{зб}), \tag{13}$$

де $C_{зб}$ – номінальне значення ємності, $\delta C_{зб}$ – відносне відхилення.

Крім того необхідно врахувати похибку від напруги зміщення нуля операційного підсилювача $U_{зм0}$:

$$\delta U_{зм0} = \frac{U_{зм}}{U_{вх.ном}}, \tag{14}$$

де $U_{вх.ном}$ – номінальне максимальне значення вхідної напруги операційного підсилювача;

$U_{зм}$ – номінальне значення напруги зсуву нуля операційного підсилювача.

Як уже зазначалось, для ідеального пристрою вибірки-зберігання $U_{вих} = U_{вх} \cdot$ Проте конденсатор в процесі зберігання розряджається, тому:

$$U_{вих} = U_{вх} \cdot (1 - \delta U_{вх}). \tag{15}$$

$$\delta U_{вх} = 1 - e^{-\frac{t_m}{\tau_p}} \tag{16}$$

де $\tau_p = R_{екв} \cdot C_{зб}$ – стала часу розрядження, (17)

t_m – тривалість одного такту.

$R_{екв} = \frac{R_{кл} \cdot R_{вх}}{R_{кл} + R_{вх}}$ – еквівалентний опір, де $R_{кл}$ – опір замкненого ключа пристрою вибірки-зберігання, $R_{вх}$ – вхідний опір ОП пристрою вибірки-зберігання.

Тобто похибку, яку вносить ПВЗ можна визначити за допомогою наступного співвідношення:

$$\Delta k^{ПВЗ} = (-e^{-\frac{t}{R_{екв} \cdot C_{зб} \cdot (1+\delta C_{зб})}}) \cdot (1 - \delta U_{зм0}^{ПВЗ}). \tag{18}$$

Підставляючи (18) у (9) можна визначити напругу на *i+1*-му кроці U'_{i+1} з урахування похибки ПВЗ:

$$U'_{i+1} = U_i \cdot \Delta k^{ПВЗ} \cdot (1 + k^{СМ}) - U_{оп}, \tag{19}$$

а похибка, яку вносить ПВЗ можна визначити за співвідношенням:

$$\delta U_{i+1}^{ПВЗ} = \frac{\left[U_i \cdot \Delta k^{ПВЗ} \cdot (1 + k^{СМ}) - U_{оп}\right] - \left[U_i \cdot (1 + k^{СМ}) - U_{оп}\right]}{U_i \cdot (1 + k^{СМ}) - U_{оп}}, \tag{20}$$

Залежність $\delta U_{i+1}^{ПВЗ}$ від номеру розряду за наявності похибки ПЗВ зображено на рис. 5.

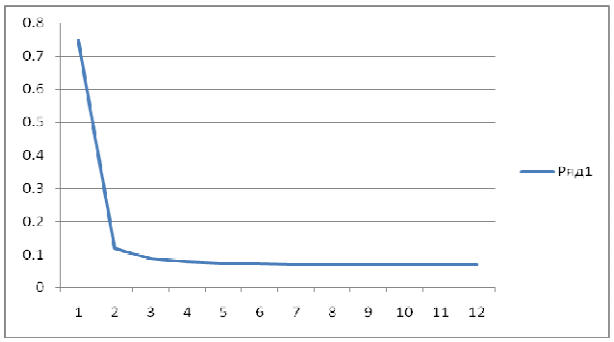


Рисунок 5 – Залежність $\delta U_{i+1}^{ПВЗ}$ від номеру розряду за наявності похибки ПВЗ

Похибки отримані на виході схем підсилення сигналу на α і схеми віднімання передусім обумовлені відхиленням резисторів від номіналу. Реальне значення резистора при наявності відхилення від номіналу визначається як R= R·(1+δR), де R – номінальне значення опору, δR – відносне відхилення. А також врахуємо похибку від напруги зміщення нуля операційного підсилювача $U_{зм0}$ яку можна обрахувати за співвідношенням (14).

Отже отримаємо залежності сигналу на виході перетворювача за наявності похибок на підсилювачі і схемі віднімання.

Для схеми підсилення сигналу на основу системи числення α враховуючи співвідношення R=R·(1+δR) та вираз (14) вирази (5) матиме вигляд:

$$U_i = U_{вх} \cdot (1 + \frac{R_2^{CM} + \Delta R_2^{CM}}{R_1^{CM} + \Delta R_1^{CM}}) \cdot (1 - \delta U_{зм0}^{CM}). \tag{21}$$

Тому похибка, яку вносить схема підсилення визначається рівнянням:

$$k^{CM} + \Delta k^{CM} = (1 + \frac{R_2^{CM} + \Delta R_2^{CM}}{R_1^{CM} + \Delta R_1^{CM}}) \cdot (1 - \delta U_{зм0}^{CM}). \tag{22}$$

Враховуючи вирази (21), (22) та підставляючи їх у вираз (9) можна визначити реальну напругу на *i+1*-му циклі U'_{i+1}:

$$U'_{i+1} = U_i \cdot (1 + k^{CM} + \Delta k^{CM}) - U_{оп}. \tag{23}$$

Похибка схеми множення:

$$\delta U_{i+1}^{CM} = \frac{\left[U_i \cdot (1 + k^{CM} + \Delta k^{CM}) - U_{оп}\right] - \left[U_i \cdot (1 + k^{CM}) - U_{оп}\right]}{U_i \cdot (1 + k^{CM}) - U_{оп}}. \tag{24}$$

Графік залежності δU_{i+1}^{CM} від номеру розряду враховуючи похибку схеми множення зображено на рис. 6.

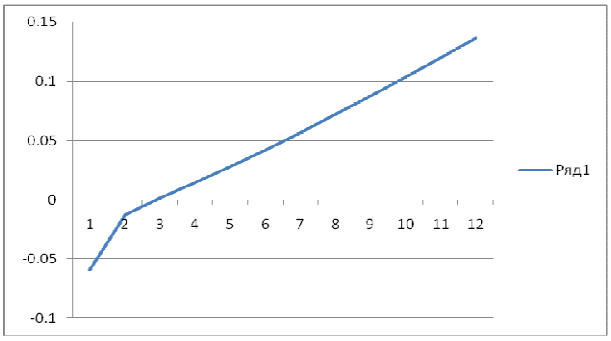


Рисунок 6 – Залежність δU_{i+1}^{CM} від номеру розряду за наявності похибки схеми множення

Відповідно похибки внесені схемою віднімання для кожного із входів можна представити рівняннями:

$$k_1^{CB} + \Delta k_1^{CB} = \frac{((R_{зз}^{CB} + \Delta R_{зз}^{CB}) + (R_1^{CB} + \Delta R_1^{CB})) \cdot (R_з^{CB} + \Delta R_з^{CB})}{((R_з^{CB} + \Delta R_з^{CB}) + (R_2^{CB} + \Delta R_2^{CB})) \cdot (R_1^{CB} + \Delta R_1^{CB})}, \quad (25)$$

$$k_2^{CB} + \Delta k_2^{CB} = \frac{R_{зз}^{CB} + \Delta R_{зз}^{CB}}{R_1^{CB} + \Delta R_1^{CB}}, \quad (26)$$

а вираз (8) набуває наступного вигляду:

$$U_i = \left(k_1^{CB} + \Delta k_1^{CB}\right) \cdot U_2 - \left(k_2^{CB} + \Delta k_2^{CB}\right) \cdot U_1. \quad (27)$$

Враховуючи вирази (25), (26) та (14) для схеми віднімання співвідношення (9) реальної реальну напруги на *i+1*-му циклі U'_{i+1} буде знаходитись за співвідношенням:

$$U'_{i+1} = \left[\left(k_1^{CB} + \Delta k_1^{CB}\right) \cdot \left(U_i \cdot (1 + k^{CM})\right) - \left(k_2^{CB} + \Delta k_1^{CB}\right) \cdot U_{on}\right] \cdot (1 - \delta U_{зм0}^{CB}), \quad (28)$$

$$\delta U_{i+1}^{CB} = \frac{\left[\left[\left(k_1^{CB} + \Delta k_1^{CB}\right) \cdot \left(U_i \cdot (1 + k^{CM})\right) - \left(k_2^{CB} + \Delta k_1^{CB}\right) \cdot U_{on}\right] \cdot (1 - \delta U_{зм0}^{CB})\right] - \left[U_i \cdot (1 + k^{CM}) - U_{on}\right]}{U_i \cdot (1 + k^{CM}) - U_{on}}. \quad (29)$$

Залежність δU_{i+1}^{CB} від номеру розряду із похибкою схеми віднімання представлено на рис. 7.

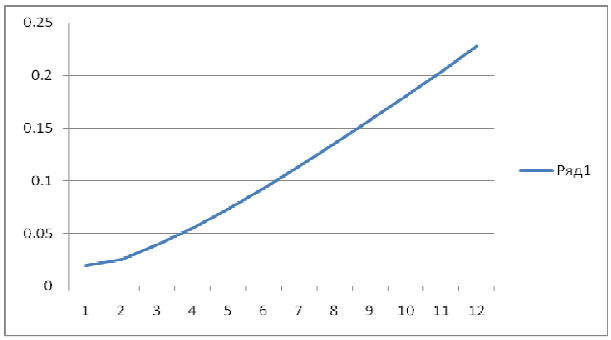


Рисунок 7 – Залежність δU_{i+1}^{CB} від номеру розряду із похибкою схеми віднімання

Відповідно вага розряду з урахуванням усіх видів похибок вираз (9) матиме вигляд:

$$U'_{i+1} = \left[\left(k_1^{CB} - \Delta k_1^{CB}\right) \cdot \left(U_i \cdot \Delta k^{ПВЗ}\right) \cdot (1 + k^{CM} + \Delta k^{CM}) - U_{on} \cdot \left(k_2^{CB} - \Delta k_2^{CB}\right)\right] \cdot (1 - \delta U_{зм0}^{CB}). \quad (30)$$

Залежність δU_{i+1} від номеру розряду за наявності усіх видів похибок можна знайти за співвідношенням:

$$\delta U_{i+1} = \frac{\left[\left[\left(k_1^{CB} - \Delta k_1^{CB}\right) \cdot \left(U_i \cdot \Delta k^{ПВЗ}\right) \cdot (1 + k^{CM} + \Delta k^{CM}) - U_{on} \cdot \left(k_2^{CB} - \Delta k_2^{CB}\right)\right] \cdot (1 - \delta U_{зм0}^{CB})\right] - \left[U_i \cdot (1 + k^{CM}) - U_{on}\right]}{U_i \cdot (1 + k^{CM}) - U_{on}}. \quad (31)$$

Залежність δU_{i+1} за наявності усіх видів похибок від номеру розряду представлено на рис. 8.

Розкривши дужки у виразі 30 отримаємо наступне співвідношення:

$$U'_{i+1} = \left[\left(k_1^{CB} - \Delta k_1^{CB}\right) \cdot \left(U_i \cdot \Delta k^{ПВЗ}\right) \cdot (1 + k^{CM} + \Delta k^{CM}) \cdot (1 - \delta U_{зм0}^{CB})\right] - \left[U_{on} \cdot \left(k_2^{CB} - \Delta k_2^{CB}\right) \cdot (1 - \delta U_{зм0}^{CB})\right] \quad (32)$$

Якщо представимо як Δ_1 похибку, яку вносять блоки у перший доданок і Δ_2 – як похибку другого доданку:

$$\Delta_1 = \left(k_1^{CB} - \Delta k_1^{CB}\right) \cdot \Delta k^{ПВЗ} \cdot (1 + k^{CM} + \Delta k^{CM}) \cdot (1 - \delta U_{зм0}^{CB}), \quad (33)$$

$$1 + \Delta_2 = \left(k_2^{CB} - \Delta k_2^{CB}\right) \cdot (1 - \delta U_{зм0}^{CB}), \quad (34)$$

то вираз (2), який описує ідеальний процес перетворення циклічного АЦП, можна представити наступним чином:

$$U_{i+1} = (\alpha + \Delta_1) \cdot U_i + (1 + \Delta_2) \cdot a_i \cdot U_{on}, \quad (35)$$

де Δ_1 – похибка, яка впливає на лінійність перетворювача,

Δ_2 – похибка, яка впливає на коефіцієнт нахилу характеристики перетворення.

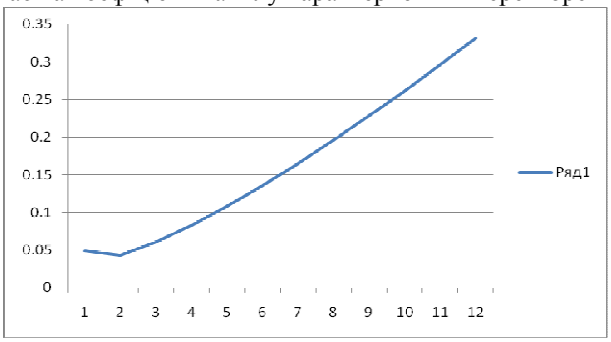


Рисунок 8 – Залежність δU_{i+1} від номеру розряду

Аналізуючи вплив кожного із блоків, що входять до циклічного АЦП, можна зробити висновок, що похибки ПВЗ і схеми множення є мультиплікативними, тобто входять до Δ_1, а похибки схеми віднімання являються адитивними і відповідно входять до Δ_2. Похибка Δ_2 призводить до зміни нахилу кодувальної характеристики і не впливає на лінійність перетворювача (рис. 9.б). Похибка Δ_1 впливає на лінійність перетворювача і призводить до появи пропуску кодів (рис. 9.в) у кодувальній характеристиці двійкового АЦП.

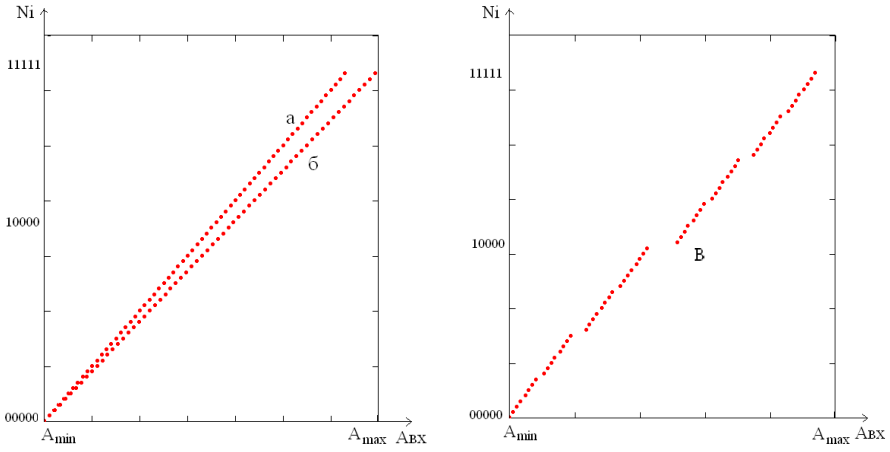
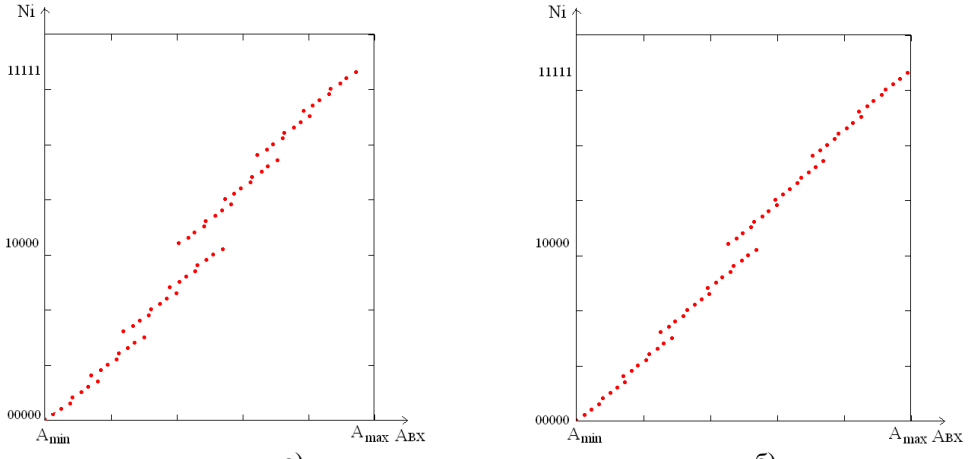


Рисунок 9 – Характеристика вхід-вихід АЦП з основою системи числення α=2:
а – АЦП з ідеальними вагами розрядів;
б – АЦП із Δ_2 =0,1; в – АЦП із Δ_1 =0,2.

Кодувальну характеристику циклічного АЦП із ваговою надлишковістю за наявністю і відсутністю відхилень ваг розрядів показано на рисунку 10а та 10б.



а) б)

Рисунок 10 – Характеристика вхід-вихід АЦП з основою системи числення
а) α=1,7, Δ_1=0, Δ_2=0; б) α=1,7, Δ_1=0,2, Δ_2=0,1

Використання НПСЧ дозволяє виключити розриви, які виникають через зазначені причини.

Висновки

У роботі розглянуто функціональні блоки, що входять до циклічного АЦП, досліджено процес утворення похибок даними блоками та приведено математичні співвідношення для їх визначення. Проведено класифікацію похибок, що дозволяє віднести їх до адитивних або мультиплікативних і показано вплив даних складових на передатну характеристику. Доведено, що похибки зміщення нуля і відхилення резисторів від номіналу схеми віднімання протягом одного такту впливають тільки на нахил кодувальної характеристики, а похибки пристрою вибірки-зберігання, схеми множення і накопичення похибок схеми віднімання змінюють робочу систему числення. Показано, що застосування вагової надлишковості дозволяє уникнути розривів кодувальної характеристики, що спричиняють похибки другої групи та відкоригувати їх методами цифрового калібрування.

Література

1. Захарченко С.М. Самокалібровані АЦП з накопиченням заряду на основі надлишкових позиційних систем числення. Монографія. / Захарченко С.М., Азаров О.Д., Харьков О.М. – Вінниця: УНІВЕРСУМ–Вінниця, 2005. – 235 с.

2. Мулявка Я. Схемы на операционных усилителях с переключаемыми конденсаторами: пер. с польск. / Мулявка Я.– Москва: МИ. – 1992. – 416с.

3. Шляндин В.М. Цифровые измерительные устройства: Учебник для вузов. / Шляндин В.М. – М.: Высшая школа, 1981. - 335 с.

4. Высокопроизводительные преобразователи формы информации / А.И. Кондалев, В.А. Багацкий, В.А. Романов, В.А. Фабричев // Наукова думка, 1987. – 280 с.

5. Алипов Н.В. Алгоритмы функционирования параллельно-последовательных преобразователей формы информации, корректирующих динамические ошибки // Автоматизированные системы управления и приборы автоматики. / Алипов Н.В. – Харьков: Вища школа. – 1985. – С. 57-64.

6. Азаров А.Д. Разработка теории аналого-цифрового преобразования на основе избыточных позиционных систем счисления: Автореф. дис… д-ра техн.наук: 05.11.16 / Азаров А.Д. / - Винницкий политехнический институт. - Винница, 1994. - 44 с.

7. Захарченко С.М. Исследование и разработка самокалибрующихся АЦП с накопителем заряда на основе избыточных позиционных систем счисления. Автореф. дис… канд. техн. наук: 05.13.08 / Захарченко С.М. / Винниц. гос. техн. ун-т. - Винница, 1997. – 16 с.

8. Стахов А.П. Аналого-цифровые преобразователи на основе избыточных систем счисления // Помехоустойчивые коды. / Стахов А.П., Азаров А.Д., Моисеев В.И. – М.: Знание, 1989. – С. 40-48.

Відомості про авторів

Захарченко Сергій Михайлович – к.т.н., доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 58-02-25.

Бойко Олександр Володимирович – аспірант кафедри обчислювальної техніки, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, e-mail: alexandr_boiko3@gmail.com.

Захарченко Галина Сергіївна – студентка, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

УДК 004.032.26

О.К. КОЛЕСНИЦЬКИЙ, С.М. ПАВЛОВ, І.В. БОКОЦЕЙ, Г.О. КОЛЕСНИЦЬКА

Вінницький національний технічний університет, Вінниця

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ІМПУЛЬСНОГО НЕЙРОЕЛЕМЕНТА НА ТИРИСТОРІ

Анотація. Запропоновано структурну схему реалізації імпульсної моделі нейрона. Згідно цієї схеми розроблено імпульсний нейронний елемент на тиристорі, який має велику навантажувальну спроможність, що дає змогу використовувати його для побудови компактних реалізацій імпульсних нейронних мереж на основі матриць світлодіодів або напівпровідникових лазерів. Наведено дані експериментальних досліджень цього нейроелемента та шляхи подальшого вдосконалення.

Ключові слова: імпульсний нейрон, тиристор, імпульсні нейронні мережі, апаратна реалізація, експериментальні дослідження.

Аннотация. Предложена структурная схема реализаци импульсной модели нейрона. Согласно этой схеме разработан импульсный нейронный элемент на тиристоре, который имеет большую нагрузочную способность, что дает возможность использовать его для построения компактных реализаций импульсных нейронных сетей на основе матриц светодиодов или полупроводниковых лазеров. Приведены данные экспериментальных исследований этого нейроэлемента и пути дальнейшего совершенствования.

Ключевые слова: импульсный нейрон, тиристор, импульсные нейронные сети, аппаратная реализация, экспериментальные исследования.

Annotation. The structure diagram of pulsed neuron model implementation is proposed. The thyristor based pulsed neural element is developed according to this structure diagram. This neural element has a big load-driving capability, that gives a possibility to use it when compact pulsed neural network constructing on the base of LED arrays or semiconductor laser diode arrays. Experimental research data and future enhancement directions of the neural element are presented.

Keywords: pulsed neuron, thyristor, pulsed neural network, hardware implementation, experimental research.

Вступ

Останнім часом штучні нейронні мережі (ШНМ) все частіше використовують в системах штучного інтелекту для розпізнавання складних динамічних образів, прогнозування багатопараметричних процесів, підтримки прийняття рішень в складних системах управління за умов невизначеності та при розв'язанні інших складних когнітивних задач, де традиційні комп'ютерні системи, що працюють за чіткими алгоритмами та програмами, виявляються неефективними [1, 2]. Однак поки що більшість практичних застосувань нейромережевих систем реалізується програмно (у вигляді комп'ютерних моделей) або програмно-апаратно (у вигляді спеціальних плат у складі традиційних комп'ютерів та програмного забезпечення для них) [1, 2].

Актуальність

Програмні та програмно-апаратні реалізації ШНМ характеризуються невеликою кількістю нейронів і використовують доволі спрощені моделі біологічних нейронів (не відтворюється велика кількість функцій нейрона), що не дозволяє досліджувати та моделювати за їх допомогою принципи роботи мозку людини для використання отриманих знань при створенні систем штучного інтелекту. Саме тому актуальною задачею є створення апаратних реалізацій нейроелементів, які відтворювали б якомога більше функцій біологічного нейрона та були б при цьому максимально простими апаратно. Саме цим критеріям відповідають імпульсні нейроелементи [2-4], в яких інформація представляється, так само як і в біологічних нейронах, частотою імпульсів. Але мало створити апаратний нейрон, потрібно, щоб він мав засоби для зручного з’єднання з великою кількістю інших нейронів. Зручність міжз’єднань забезпечується при використанні оптичних сигналів як носіїв інформації, тому створювані імпульсні нейроелементи мають бути оптоелектронними. Крім цього, як показано в роботі [5], для зменшення масо-габаритних показників нейромереж, імпульсні нейроелементи повинні мати велику навантажувальну спроможність, щоб керувати одразу рядком (стовпчиком) матриці світлодіодів або напівпровідникових лазерів.

Мета

Мета цієї статті - висвітлити запропоновану авторами апаратну реалізацію імпульсного нейрона на основі тиристора, навести результати його експериментальних досліджень, провести аналіз досяжних параметрів та характеристик, визначити напрямки подальших досліджень.

Постановка задачі

Необхідно створити апаратні реалізації імпульсної моделі нейрона (імпульсні нейроелементи), які повинні мати оптичні входи-виходи для забезпечення зручності міжз’єднань в мережі та повинні мати велику навантажувальну спроможність, щоб керувати одразу рядком (стовпчиком) матриці світлодіодів або напівпровідникових лазерів та експериментально дослідити їх експлуатаційні параметри та характеристики..

Розв'язання задач

1. Імпульсна модель нейрона

У відомих нейроелементах [3] інформаційним носієм можуть бути: цифрові коди, часові інтервали, струм, напруга, імпульсні сигнали. Як відомо з фізіології, в нейронах мозку інформація передається в імпульсній формі, тому саме імпульсні моделі нейрона є найбільш адекватними до біологічних нейронів і їх дослідження є вельми актуальною задачею.

При розробці структурної схеми імпульсної моделі нейрона потрібно виконати наступні вимоги:

1) імпульсна модель нейрона по набору своїх функцій повинна бути максимально адекватною біологічному нейрону;

2) з урахуванням подальшого використання в оптоелектронних нейронних мережах, де сигнали між нейронами передаються в оптичному вигляді, імпульсна модель нейрона повинна мати оптичні входи і виходи;

3) оскільки вхідні сигнали нейронів повинні інтегруватись (додаватись) в нейроні, то в якості такого інтегратора доцільно взяти електричну ємність;

4) для виконання порогової обробки накопичених вхідних сигналів, в схемі імпульсної моделі нейрона має бути пороговий пристрій;

5) для формування вихідного імпульсу певної тривалості має бути коло розряду інтегратора (ємності).

На рис. 1 наведено структурну схему реалізації імпульсної моделі нейрона.

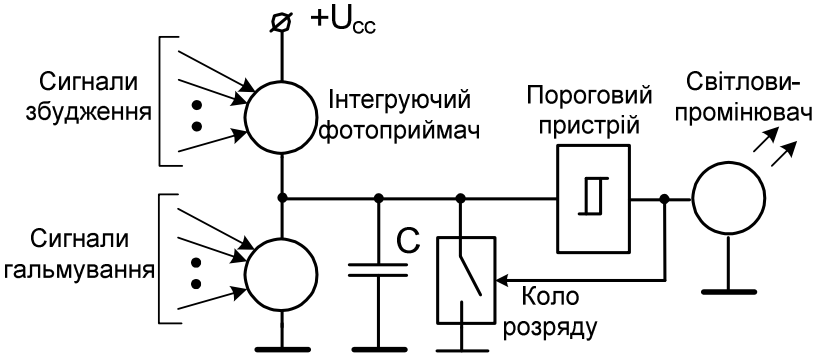


Рисунок 1 – Структурна схема реалізації імпульсної моделі нейрона

Вона має оптичні входи (збуджувальні та гальмівні), які подаються на відповідні фотоприймачі. Алгебраїчна сума фотострумів з цих фотоприймачів інтегрується на ємності С. При досягненні різницею потенціалів на ємності порогової величини, спрацьовує пороговий пристрій, формуючи на своєму виході передній фронт вихідного імпульсу. По цьому передньому фронту включається коло розряду ємності, від параметрів якого залежить тривалість вихідного імпульсу. Для забезпечення оптичного виходу, в схему введено світловипромінювач.

Пороговий пристрій може бути реалізований на різних елементах. Це можуть бути напівпровідникові прилади з ділянкою від'ємного опору на ВАХ: тиристори, тунельні діоди, одноперехідні транзистори, біспін-прилади [2]; а також напівпровідникові прилади з пороговими властивостями: лавинний транзистор, стабілітрон; порогові схеми на біполярних або МОН-транзисторах зі зворотними зв'язками. В цій статті пропонується реалізація імпульсної моделі нейрона з пороговим пристроєм на тиристорі [4].

2. Апаратна реалізація імпульсної моделі нейрона на тиристорі

Для апаратної реалізація структурної схеми імпульсної моделі нейрона (див. рис. 1), було обрано варіант виконання порогового пристрою на основі тиристора. Цей вибір визначається тим, що тиристор може керувати (перемикати) великими струмами. Саме ця властивість необхідна для того, щоб нейроелемент міг керувати одразу лінійкою матриці світлодіодів або напівпровідникових лазерів. Маючи такі нейроелементи, можна будувати апаратні реалізації нейронних мереж на основі матриць світлодіодів або напівпровідникових лазерів у вигляді «сендвіч-структур» [4] з покращеними масо-габаритними показниками.

Прототипом запропонованому нейроелемента на тиристорі є пристрій [6], який містить просторово-часовий суматор вхідних сигналів (виконаний на конденсаторі), генератор імпульсів на тиристорі з резистивно-ємнісними ланками в катодному та анодному ланцюгах. Крім того, пристрій містить розділювальні напівпровідникові діоди та резистор для встановлення режиму роботи пристрою (режими очікування або спонтанної активності). Недоліком даного пристрою є електрична природа вхідних та

вихідних сигналів (що ускладнює технологію побудови на таких елементах нейронних мереж з великою кількістю міжз’єднань) та відсутність гальмівних входів (що обмежує функціональні можливості пристрою). Задачею вдосконалення пристрою для моделювання нейрона (нейроелемента) [6] було забезпечення можливості пристрою працювати з оптичними сигналами та наявність як збуджувальних, так і гальмівних входів, що розширює функціональні можливості пристрою.

На рис. 2 наведено схему запропонованого [4] нейроелемента. Нейроелемент містить перший VD1 та другий VD2 фотодіоди, конденсатор C1 для просторово-часового підсумовування, генератор імпульсів, що виконаний на тиристорі VS1 з резистором R3, світловипромінювачем VD3 та конденсатором C2 в катодному ланцюгу і резистором R2 та конденсатором C3 в анодному ланцюгу, резистор R1 для встановлення режиму роботи нейроелемента (очікування або фонової активності), електричний вихід та оптичний вихід (на VD3), а також збуджувальний (на VD1) та гальмівний (на VD2) входи нейроелемента.

Нейроелемент працює таким чином. Перший фотодіод VD1 приймає збуджувальні вхідні оптичні сигнали, які перетворюються фотодіодом в струм, що заряджає конденсатор C1. Другий фотодіод VD2 приймає гальмівні вхідні оптичні сигнали, які перетворюються фотодіодом VD2 в струм, що розряджає конденсатор C1. Напруга живлення тиристора менша напруги його перемикання при струмі керуючого електрода, що регулюється резистором R1 (в режимі очікування). Коли напруга на керуючому електроді тиристора під дією вхідних імпульсів досягне порогового значення (при даній напрузі живлення), тиристор відкривається, на резисторі R3 і світловипромінювачі VD3 створюється вихідний позитивний імпульс напруги, який надходить на електричний вихід (світловипромінювач VD3 формує в цей час вихідний оптичний імпульс). Конденсатор C3 розряджається через відкритий тиристор, резистор R3 і світловипромінювач VD3, напруга на аноді тиристора зменшується і він закривається. Конденсатор C2, що зарядився під час відкритого стану тиристора, розряджається через резистор R3 і світловипромінювач VD3, формуючи задній фронт вихідного імпульсу. Після замикання тиристора конденсатор C3 заряджається від джерела напруги через резистор R2 до початкового значення, моделюючи фазу пониження збудження (відносна рефрактерність).

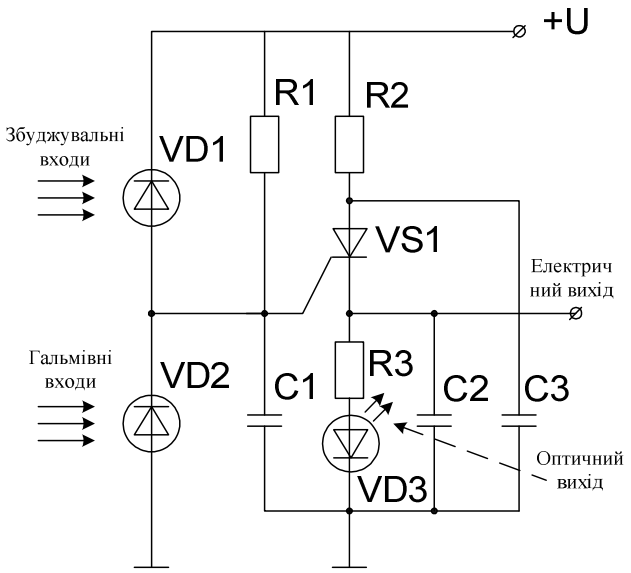


Рисунок 2 – Нейроелемент на тиристорі

Завдяки наявності оптичних входів та виходів даний нейроелемент може легко використовуватись при побудові імпульсних нейронних мереж з великою кількістю елементів та зв’язків між ними. Організація великої кількості оптичних зв’язків реалізується набагато простіше, ніж електричних зв’язків за допомогою оптичних та голографічних засобів. Крім того, завдяки тому, що тиристор може перемикати великі струми, як світловипромінювач VD3 може використовуватись кілька паралельно з’єднаних світлодіодів або напівпровідникових лазерів. Це дає змогу навантажувати нейроелемент на цілий рядок або стовпчик матриці світлодіодів або напівпровідникових лазерів, що спрощує структуру побудови великих нейронних мереж, де один нейрон повинен передавати свій вихідний сигнал на всі інші нейрони. Наявність в запропонованому нейроелементі крім збуджувальних також і гальмівних входів підвищує адекватність нейроелемента своєму біологічному прототипу та дозволяє організовувати нейронні мережі як з додатними, так і з від’ємними коефіцієнтами синаптичних зв’язків (що розширює функціональні можливості).

Якщо як тиристор використати світловипромінюючий тиристор, то тоді світловипромінювач VD3 можна виключити зі схеми, а оптичним виходом нейроелемента буде апертура світловипромінюючого тиристора.

3. Експериментальні дослідження імпульсного нейроелемента на тиристорі

Для експериментальної перевірки працездатності запропонованого нейроелемента був зібраний експериментальний макет, схема якого показана на рис. 3. За допомогою фотодіодних оптопар *VU*1 і *VU*2 (тип АОД109Б) моделювалася дія оптичних потужностей $P_{зб}$ і $P_{глм}$ відповідно збуджувальних та гальмівних вхідних оптичних сигналів нейрона. За допомогою джерел постійної напруги *G*1 і *G*2 (Б5-49), а також резисторів *R*1 і *R*2 змінювався струм в колі світлодіодів оптопар. Струм світлодіодів оптопар контролювався мікроамперметром (вольтметр універсальний В7-21а — на схемі рис. 3 не показаний).

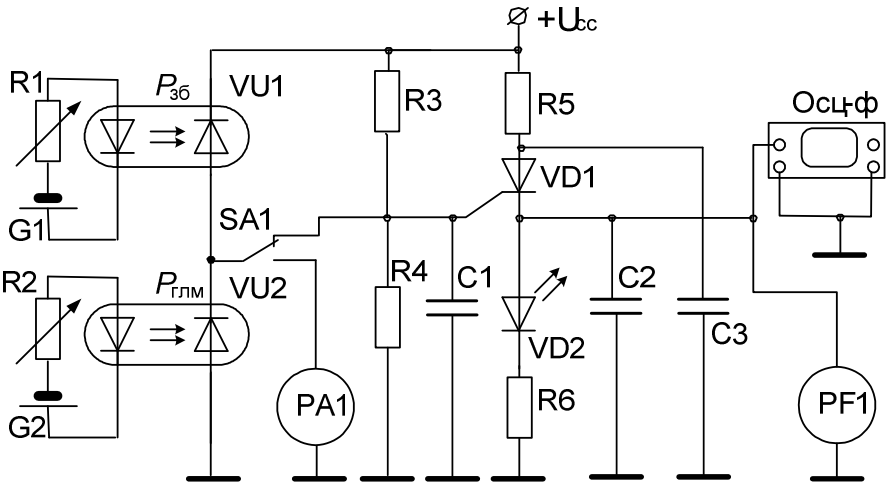


Рисунок 3 – Схема експериментального макету для дослідження імпульсного нейроелемента на тиристорі

Перемикач SA1 служить для перемикання нейроелементу з режиму вимірювання сумарного фотоструму фотодіодів оптопар (на мікроамперметрі PA1 — вольтметр універсальний В7-21а) у робочий режим. У робочому режимі вихідні імпульси контролювалися за допомогою осцилографа (С1-93), а їх частота вимірювалася за допомогою частотоміра PF1. Параметри схеми: *C*1=*C*2=*C*3=0,01 мкф, *R*5=1 кОм, *R*6=1 кОм, *VD*1 – тиристор КУ112А, *VD*2 – світлодіод АЛ307Б.

Експериментальні дослідження нейроелемента проводилися таким чином. Напруга живлення складала $U_{сс}$=12 В. Резистори *R*3 та *R*4 підбирались так, щоб при відсутності вхідних сигналів на виході нейроелемента спостерігалась нестійка імпульсація. Наприклад, при *R*3=34 кОм, імпульсація починалась при *R*4=11,5 кОм і закінчувалась при *R*4=16,9 кОм (тиристор переходив у відкритий стан). Було проведено 2 експерименти для 2 фіксованих значень оптичної потужності на гальмівному вході $P_{глм}$ (фіксовані значення оптичної потужності відповідають таким фотострумам: $I_{глм1}$=0, $I_{глм2}$=100 мкА). У кожному з 2 експериментів оптична потужність $P_{зб}$ на збуджувальному вході змінювалася від 0 до 580 мкВт (що відповідає зміні фотоструму $I_{зб}$ через фотодіод оптопари VU1 від 0 до 310 мкА). Графіки цих залежностей представлені на рис. 4.

Логічно виникло питання: як впливають номінали *R*3 та *R*4 на діапазони вхідних фотострумів, вихідних частот та параметри вихідних імпульсів. Виявилось, що номінали *R*3 та *R*4 майже не впливають на параметри вихідних імпульсів, суттєво впливають на діапазон вхідних фотострумів та майже не впливають на діапазон вихідних частот.

Для з'ясування величини впливу на діапазон вхідних фотострумів, експериментально були підібрані *R*3 та *R*4, при яких діапазон вхідних фотострумів виявився максимальним. Вони виявилися такі: *R*3=1 кОм, *R*4=2,5 кОм. Було проведено 2 експерименти для 2 фіксованих значень оптичної потужності на гальмівному вході $P_{глм}$ (фіксовані значення оптичної потужності $P_{глм}$ відповідають таким фотострумам: $I_{глм1}$ = 0, $I_{глм2}$ = 1,8 мА). В кожному з 2 експериментів оптична потужність на вході збудження змінювалася від 0 до 10,3 мВт (що відповідає зміні фотоструму через фотодіод оптопари VU1 від 0 до 5,5 мА). Графіки цих залежностей представлені на рис. 5.

Із рис. 4 та рис. 5 видно, що при зміні *R*3=34 кОм, *R*4=9,1 кОм на *R*3=1 кОм, *R*4=2,5 кОм, діапазон вихідних частот майже не змінився (був 0…7,7 кГц, став 0…9,8 кГц), а діапазон вхідних фотострумів (оптичних потужностей) розширився (був 0…350 мкА, став 0…6500 мкА).

Також було цікаво дослідити як схема працює на низькоомне навантаження (тобто коли навантаження еквівалентне рядку матриці світлодіодів). Тому було проведено експеримент при *R*6=45,8 Ом (без

*VD*2). при $I_{глм} = 0$. В експерименті оптична потужність на вході збудження змінювалася від 0 до 20,6 мВт (що відповідає зміні фотоструму через фотодіод оптопари VU1 від 0 до 11 мА). Результати експериментів у вигляді графіка наведено на рис. 6.

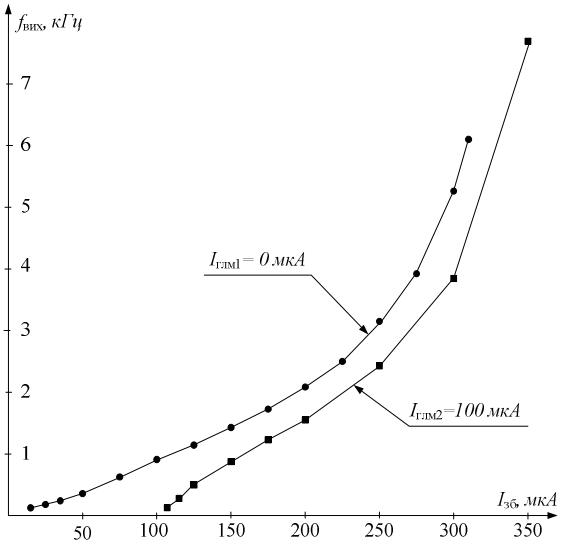


Рисунок 4 – Графіки залежностей вихідної частоти нейроелемента на тиристорі від фотоструму $I_{зб}$ збудження при $I_{глм1} = 0$ мкА, $I_{глм2} = 100$ мкА, $R3$=34 кОм, $R4$=9,1 кОм, U_{cc}=12 В

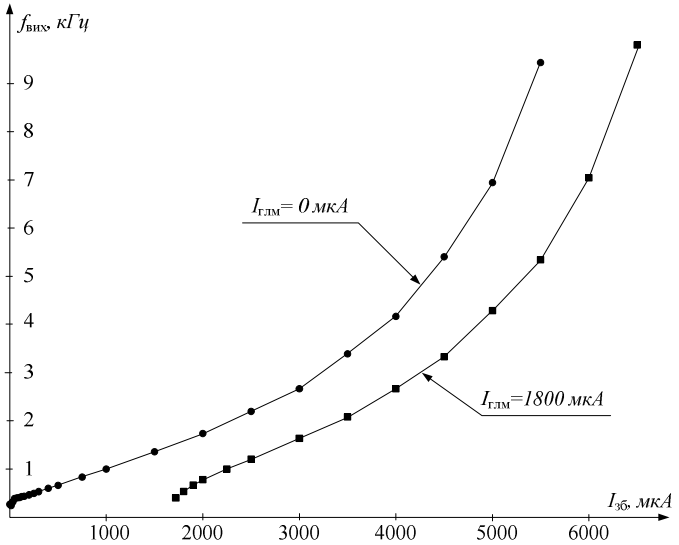


Рисунок 5 – Графіки залежностей вихідної частоти нейроелемента на тиристорі від фотоструму $I_{зб}$ збудження при $I_{глм1} = 0$ мкА, $I_{глм2} = 1800$ мкА, $R3$=1 кОм, $R4$=2,5 кОм, U_{cc}=12 В

Форма вихідних імпульсів нейроелемента на тиристорі представлена на рис. 7, причому на рис. 7а – форма імпульсу при невеликих значеннях вхідної оптичної потужності (фотоструму $I_{зб}$) , а на рис. 7б – при великих значеннях $I_{зб}$. Тобто видно, що при збільшенні вхідної оптичної потужності (фотоструму $I_{зб}$), максимальне значення амплітуди U_{Amax} зменшується , а мінімальне U_{Amin} – збільшується. Характер цієї залежності для параметрів схеми згідно рис. 6 представлено на рис. 8.

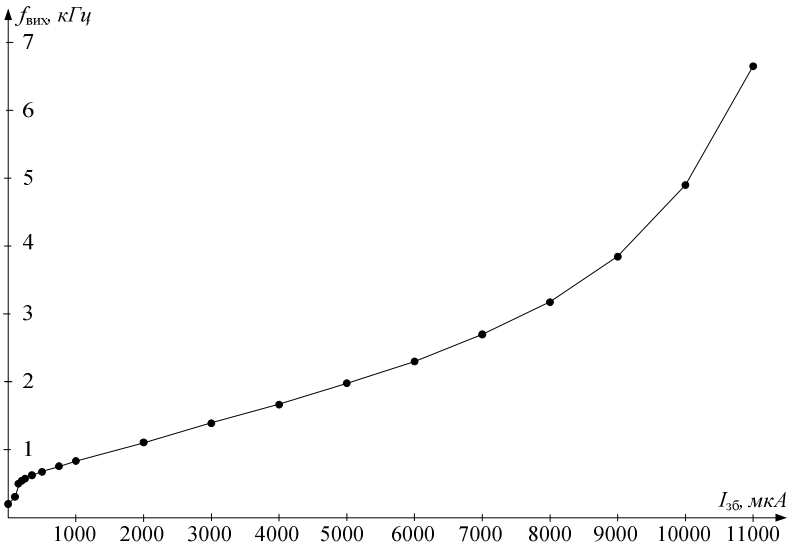
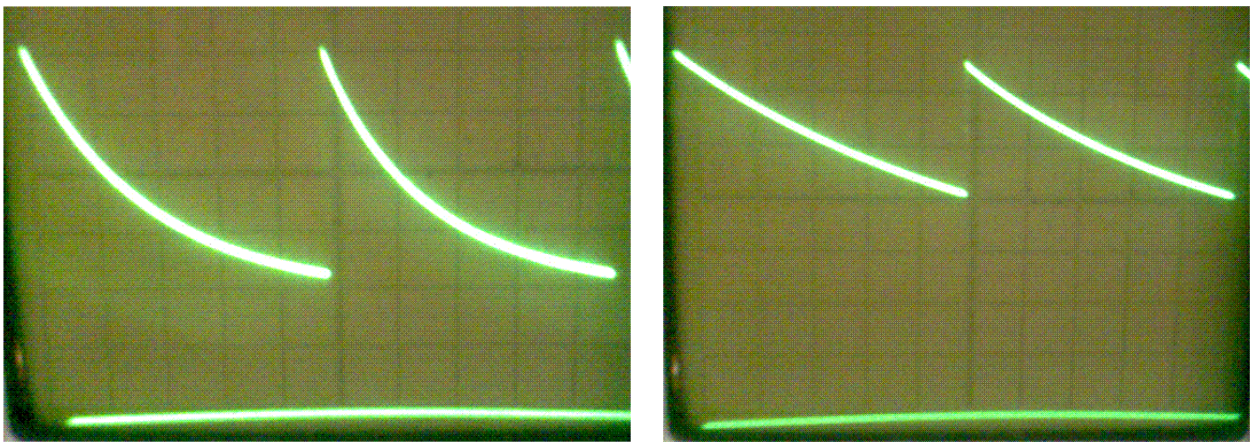


Рисунок 6 – Графік залежностей вихідної частоти нейроелемента на тиристорі від фотоструму $I_{зб}$ збудження при $I_{глм} = 0$ мкА, $R3$=1 кОм, $R4$=2,5 кОм, $R6$=45,8 Ом (без *VD*2).

Що стосується часових параметрів вихідних імпульсів, то з рис. 7 видно, що передній фронт імпульсу короткий (0,5 мкс), а задній фронт затягнутий, що викликано великим часом вимикання тиристору. Взагалі, ширина вихідного імпульсу по рівню 0,5 – порядку 250 мкс, а по рівню 0,1 – 850…900 мкс. Така велика тривалість заднього фронту імпульсу є недоліком, тому треба застосовувати або спеціальні схеми для швидкого вимикання тиристору або більш сучасні види тиристорів, наприклад, тиристори з польовим управлінням [7] (див. рис. 9).

Таким чином, в результаті експериментальних досліджень було підтверджено працездатність запропонованого [4] нейроелемента на тиристорі і набуто числових значень його основних параметрів, які зведено до табл. 1.



а) б)

Рисунок 7 – Форма вихідних імпульсів нейроелемента на тиристорі при $I_{зб}$=150 мкА, $R3$=34 кОм, $R4$=9,1 кОм, U_{cc}=12 В

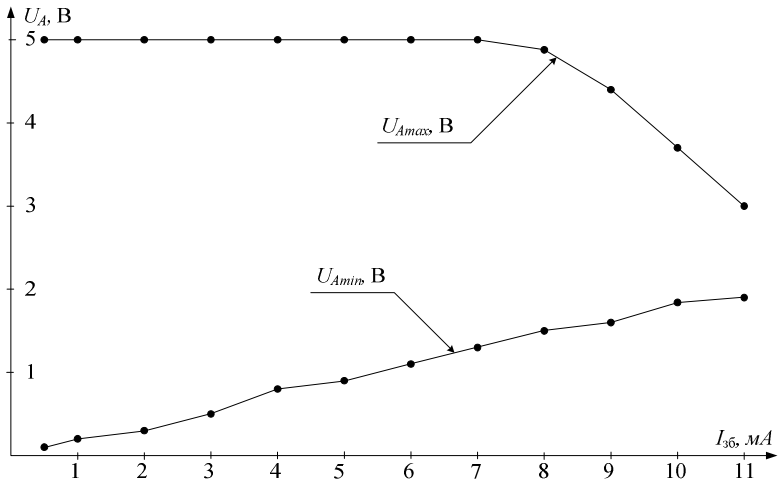


Рисунок 8 – Розмах амплітуди вихідних імпульсів нейроелемента на тиристорі при $R3$=1 кОм, $R4$=45,8 Ом, U_{cc}=12 В

Таблиця 1 – Числові значення основних параметрів нейроелемента на тиристорі

Назва параметра	Позначення	Значення параметра
Діапазон вхідних оптичних потужностей [мВт]	$P_{min}...P_{max}$	0…20
Діапазон вихідних частот [кГц]	$f_{min}...f_{max}$	0…10
Тривалість переднього фронту вихідного імпульсу [мкс]	t_{01}	0,5
Тривалість заднього фронту вихідного імпульсу [мкс]	t_{10}	800
Тривалість вихідного імпульсу по рівню 0,1 [мкс]	τ_{90}	850…900
Тривалість вихідного імпульсу по рівню 0,5 [мкс]	τ_{50}	250
Питома споживана потужність [мВт]	$P_{\text{С пит}}$	360
Комутаційні втрати [мВт]	ΔP_K	155

Експериментальні дослідження виявили недоліки нейроелемента на тиристорі, які полягають в наступному:

1) вихідні імпульси мають затягнутий задній фронт, що відрізняє форму імпульсів нейроелемента на тиристорі від форми імпульсів біологічного нейрона,

2) погана лінійність передатної характеристики (див. рис. 4-6), особливо при великих значеннях сигнала збудження, причому похідна передатної характеристики зростає, хоча краще б вона зменшувалась (це більше відповідало б такій властивості нейрона як аккомодація),

3) при низькоомному навантажені для ввімкненя тиристора потрібно, щоб *R*4 теж був низькоомним, а це значить, що буде великий паразитний струм розряду конденсатора *C*1 (див. рис. 2), що спричинить не зовсім вірну роботу нейроелемента при імпульсних вхідних сигналах,

4) схема має великі комутаційні втрати через наявність резистора *R*5 (див. рис. 2) та відносно великі струми закритого тиристора при струмах керуючого електрода, близьких до порогового,

5) хоча діапазон вихідних частот нейроелемента на тиристорі (0…10 кГц) краще, ніж у біологічних нейронів (0…2 кГц), все-одно через великий час вимикання тиристорів, слід реалізовувати імпульсні нейроелементи по структурно-функціональній моделі згідно рис. 1 на більш швидкодіючих напівпровідникових приладах з пороговими властивостями.

Щоб уникнути цих недоліків, потрібно в подальшому вдосконалити схему цього нейроелемента за рахунок використання нового типу тиристорів – тиристорів з польовим управлінням [7], які являють собою вдосконалення звичайного тиристора, що полягає у використанні для комутації струму пари МОН-транзисторів (рис. 9). Тиристори з польовим управлінням, порівняно зі звичайними тиристорами, мають більшу швидкодію (час затримки 300 нс), менш критичні до швидкості наростання струму, керуються набагато меншими струмами, мають більшу щільність струму, мале пряме падіння напруги у відкритому стані (~1,1 В), менші комутаційні втрати, можуть працювати паралельно.

Крім цього, інший шлях покращення параметрів імпульсних нейроелементів - будувати нейроелементи за схемою по рис.1 на основі інших (на відміну від тиристорів) порогових напівпровідникових пристроїв – біспін-приладів, лавинних транзисторів та ін.. Необхідну навантажувальну спроможність в цьому випадку можна досягти, під’єднавши до виходу біспін-приладу (лавинного транзистора або ін.) потужний біполярний чи польовий транзистор. А ще краще використовувати так звані біполярні транзистори з ізольованим затвором - БТІЗ [8] (Insulated Gate Bipolar Transistor - IGBT). IGBT-прилад являє собою біполярний *p*-*n*-*p*-транзистор, що керується від порівняно низьковольтного MOSFET-транзистору з індукованим каналом (рис. 10 а). Умовне позначення IGBT-приладу показано на рис. 10 б.

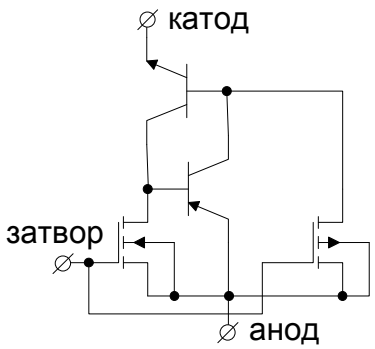


Рисунок 9 – Тиристор з польовим управлінням

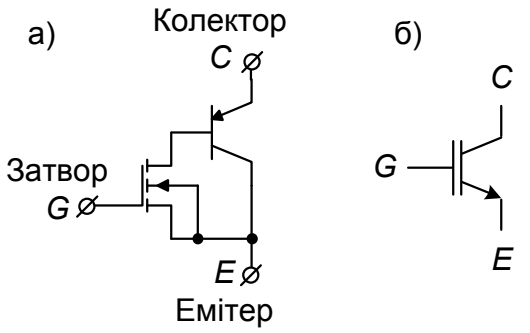


Рисунок 10 – Біполярний транзистор з ізольованим затвором (IGBT):
а) внутрішня структура IGBT-приладу,
б) умовне позначення IGBT-приладу.

IGBT-прилади є компромісним технічним рішенням, яке дозволило об’єднати позитивні якості як біполярних (мале падіння напруги у відкритому стані, високі напруги комутації), так і MOSFET-транзисторів (мала потужність управління, високі швидкості комутації). В той же час втрати у них зростають пропорційно струму, а не квадрату струму, як у польових транзисторів. Максимальну напругу IGBT-транзисторів обмежено тільки технологічним пробоєм і вже сьогодні випускаються прилади з робочою напругою до 4000 В. При цьому залишкова напруга на транзисторі у ввімкненому стані не перевищує 2…3 В.

Висновки

Таким чином, в статті запропоновано структурну схему реалізації імпульсної моделі нейрона. Згідно цієї схеми розроблено імпульсний нейронний елемент на тиристорі [4], який має велику навантажувальну спроможність, що дає змогу використовувати його для побудови компактних реалізацій імпульсних нейронних мереж [5] на основі матриць світлодіодів або напівпровідникових лазерів. Однак експериментальні дослідження цього нейроелемента виявили низку його недоліків: велика тривалість заднього

фронту вихідного імпульсу; погана лінійність передатної характеристики; великі комутаційні втрати; великі паразитні струми витікання з накопичувального конденсатора. В подальшому потрібно вдосконалити схему цього нейроелемента за рахунок використання тиристорів з польовим управлінням [7], або будувати нейроелементи за схемою по рис.1 на основі інших порогових напівпровідникових пристроїв – біспін-приладів, лавинних транзисторів та ін. із застосуванням для підвищення навантажувальної спроможності біполярних транзисторів з ізольованим затвором - БТІЗ [8] (IGBT-транзисторів).

Список літератури

1. Галушкин А.И. Нейрокомпьютеры. Кн.3: Учебное пособие для вузов/ Общая редакция А.И.Галушкина. – М.: ИПРЖР, 2000. -528с.
2. Бардаченко В. Ф. Таймерні нейронні елементи та структури. Монографія / В. Ф. Бардаченко, О. К. Колесницький, С. А. Василецький. - Вінниця : УНІВЕРСУМ-Вінниця, 2005, 126 с.
3. Колесницький О. К. Пристрої для моделювання нейрона. Аналітичний огляд винаходів та патентів / О. К. Колесницький, І. В. Бокоцей, С. С. Яремчук // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2010. – №2. – С.23-31.
4. Пат. 55921 Україна, МПК G 06 G 7/00. Пристрій для моделювання нейрона / О. К. Колесницький, І. В. Бокоцей, С. М. Павлов, Г. О. Колесницька, заявник і власник патенту Вінницьк. нац. технічн. ун-т – № 201008531; заявлено 08.07.09; опубл. 27.12.10, Бюл.№24.
5. Колесницкий О. К. Компактна оптоелектронна реалізація імпульсної нейронної мережі / О. К. Колесницкий, І. В. Бокоцей // Оптико-електронні інформаційно-енергетичні технології. – 2010. – №2. – С.54-62.
6. А.с. 376787 СССР, МКИ3 G 06 F 7/60. Устройство для моделирования нейрона / Снежко Е.М. – № 1661157; заявлено 31.05.71; опубл. 05.04.73. Бюл.№17.
7. Нестеров С. А. Тиристоры с полевым управлением / С. А. Нестеров, Тетюшкин В. С. // Электронное научное издание "Электроника и информационные технологии", №1, 2010 [Електронний ресурс]. — Режим доступу: http://www.fetmag.mrsu.ru/2010-1/pdf/Field-controlled_Thyristors.pdf.
8. Биполярный транзистор с изолированным затвором [Електронний ресурс]. — Режим доступу: http://www.texnic.ru/books/opis/sil_el/sil_el001.htm

Відомості про авторів

Колесницький Олег Костянтинович – докторант кафедри комп'ютерних наук, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 59-88-32, okk_vin@mail.ru

Павлов Сергій Миколайович – доцент кафедри проектування комп'ютерної та телекомунікаційної апаратури (ПКТА), Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

Бокоцей Ірина Віталіївна – аспірант кафедри комп'ютерних наук, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

Колесницька Ганна Олегівна – студент кафедри проектування комп'ютерної та телекомунікаційної апаратури (ПКТА), Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

УДК 681.396

В.М. КИЧАК, С.Г. БОРТНИК , Н.О. ПУНЧЕНКО

Вінницький національний технічний університет, м. Вінниця

МЕТОД ВИЗНАЧЕННЯ ХАРАКТЕРИСТИКИ ПЕРЕТВОРЕННЯ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЮВАЧА У ДИНАМІЧНОМУ РЕЖИМІ

Вступ

Одним з важливих напрямків цифрової вимірювальної техніки є створення та використання аналого-цифрових перетворювачів (АЦП), які є складовими частинами інформаційно-вимірювальних систем, інформаційно-обчислювальних комплексів, різних вимірювальних засобів і приладів. Для вирішення питання щодо використання конкретного АЦП у тій чи в іншій задачі необхідно визначити статичні та динамічні характеристики. Існує ряд методів визначення характеристик перетворення (ХП) АЦП [1]. Переважна більшість з них використовує як тестові постійні рівні напруг (лише амплітудно-частотна характеристика визначається на базі синусоїди). Очевидно, що для оцінювання якості функціонування АЦП при перетворенні швидкоплинних процесів недостатньо знати лише статичні характеристики. У більшості випадків необхідно визначати ХП АЦП у динамічному режимі.

Подальше підвищення точності АЦП у динамічному режимі стримується відсутністю ефективних методів визначення динамічних характеристик АЦП. У зв`язку з цим задача розроблення методу визначення характеристик перетворення АЦП у динамічному режимі є актуальною.

Аналіз публікацій

Основи вимірювань динамічних характеристик було закладено в роботах [1-3]. Складною задачею при визначенні ХП АЦП у динамічному режимі є забезпечення високої продуктивності методу при збереженні адекватності експерименту реальним умовам експлуатації АЦП. Ця мета при забезпеченні деяких умов, які будуть розглянуті нижче, може бути досягнута статистичним методом. Статистичний метод відноситься до методів, що направлені на визначення параметрів ХП, і тому ДХ АЦП, які визначаються за допомогою даного методу залежать від досліджуваного сигналу. На практиці, при статистичному методі переважно як тестовий використовують гармонічний сигнал. Таку тенденцію можна пояснити наявністю атестованих генераторів гармонічних сигналів та їх доступністю, а також існуванням історично сформованих методів дослідження лінійних систем.

Статистична методологія визначення ХП АЦП полягає у накопиченні великої кількості вихідних відліків АЦП з подальшим їх статистичним аналізом. Методи статистичних випробувань базуються на побудові гістограми вихідних кодів АЦП. ХП АЦП у динамічному режимі та параметри АЦП: монотонність, інтегральну та диференціальну нелінійність, можна визначити за накопиченим статистичним рядом кодових значень тестового сигналу перетворювача. При цьому знаходять розподіл частотостей вихідних кодів АЦП та апроксимувальну цей розподіл функцію густини ймовірностей. Умовами коректного випробування АЦП є незалежність та випадковість моментів часу дискретизації тестового сигналу. Як тестові впливи у гістограмних методах використовують трикутні чи синусоїдальні сигнали [4].

При дослідженні ХП АЦП гістограмним методом як вхідний частіше використовують синусоїдальний, а не трикутний сигнал. При відповідній фільтрації можна сформувати синусоїду з низьким рівнем нелінійних спотворень та шумів. На відміну від трикутного сигналу, ймовірність появи кодів для синусоїдального сигналу неоднакова. Для *n*-розрядного АЦП з повномасштабним діапазоном $\pm U_{FS}$ та вхідним синусоїдальним сигналом U_M імовірність появи *i*-го коду дорівнює [4]

$$p(i) = \frac{1}{\pi}\left[\arcsin\left(\frac{U_{FS}(i-2^{n-1})}{U_M 2^n}\right) - \arcsin\left(\frac{U_{FS}(i-1-2^{n-1})}{U_M 2^n}\right)\right]. \quad (1)$$

Для такого сигналу ймовірність появи кодів зростає при пікових значеннях синусоїди поблизу $\pm U_{FS}$, тому що крутість сигналу у цих точках приймає мінімальні значення. Для такого вхідного сигналу теоретична кількість появи *i*-го коду дорівнює

$$h_t(i) = p(i)M\,. \quad (2)$$

Відповідна диференціальна нелінійність для даного рівня квантування дорівнює

$$\delta_{LD}(i) = \frac{h_r(i)}{p(i)M} - 1\,. \quad (3)$$

Для підвищення коректності гістограмного тестування необхідно, щоб частота синусоїди не була субгармонікою частоти дискретизації. Амплітуду синусоїдального коливання слід вибирати такою, щоб АЦП був незначно перевантажений за межами діапазону вхідних напруг.

Нелінійність характеристики АЦП є чинником, що значно ускладнює дослідження. Гармонічний сигнал є одночастотним сигналом. Нехай проводиться дослідження АЦП на базі синусоїдального сигналу зі сканувальними частотами ω_1, ω_2, ... ω_K і для кожної з частот похибка перетворення не перевищує задані допустимі значення. За результатами вимірювань робиться висновок, що частотний діапазон (ω_H, ω_B) є робочим діапазоном АЦП. Очевидно, що такий висновок некоректний, тому що в реальних умовах експлуатації АЦП перетворює сигнали, які мають багатий спектральній склад. Через порушення принципу суперпозиції для нелінійних систем, похибка перетворення спектрально багатого сигналу може перевищувати похибку, що виявлена при вимірюваннях на одночастотних сигналах.

Мета дослідження

Мета дослідження полягає у розробленні високопродуктивного методу визначення ХП АЦП у динамічному режимі, що характеризується високою адекватністю отриманих результатів.

Постановка задачі

Для досягнення зазначеної мети необхідно розв'язати такі задачі:
здійснити вибір та обґрунтування тестового сигналу АЦП;
провести дослідження властивостей тестового сигналу;
розробити статистичний метод визначення ХП АЦП;
визначити продуктивність розробленого методу.

Дослідження тестового сигналу АЦП

З метою створення умов для визначення характеристик АЦП в динаміці, адекватних умовам їх експлуатації як сигнал випробування пропонується використати псевдовипадковий сигнал (ПВС). Такий сигнал має переваги випадкових (багатий енергетичний спектр) і детермінованих (можливість контролю форми) сигналів.

З широкого класу ПВС було обрано сигнал, який представляє собою послідовність імпульсів трикутної форми постійної амплітуди, але випадкової тривалості. Ця послідовність трикутних імпульсів з випадковою тривалістю (ПТІВТ) окрім оптимальних енергетичних властивостей має ще одну дуже важливу особливість: її значення розподілені рівномірно у діапазоні зміни амплітуди сигналу і при цьому не виникає ефекту "биття", характерного для періодичних тестових сигналів і пов'язаного з кратністю сигналу та періоду стробування АЦП. Для такого тестового сигналу частота дискретизації АЦП задається згідно вимог теореми Котельникова, при цьому враховуються вищі гармоніки ПТІВТ, що дає можливість послабити ефект накладання спектрів.

Фрагмент ПТІВТ довжиною N імпульсів має вигляд:

$$U^N(t) = \sum_{i=1}^{N} U_i(t) . \tag{4}$$

В інтервалі $t \in (T_{i-1}, T_i]$ трикутний імпульс з крутістю υ дорівнює

$$U_i(t) = (-1)^i \left[1 - \upsilon_i (t - T_{i-1})\right] , \tag{5}$$

де T_i - момент виникнення *i*-го імпульсу.

При використанні періодичного досліджуваного сигналу для вимірювання ХП АЦП з'являється явище "биття", пов'язане з кратністю періоду сигналу випробування та періоду дискретизації. Через один або декілька періодів тестового сигналу вихідна послідовність відліків АЦП також періодизується. Деякі кодові комбінації АЦП при цьому просто не тестуються, тому що імпульс дискретизації не попадає на ділянки аналогового сигналу, які відповідають цим кодовим комбінаціям. При цьому неможливо визначити з чим пов'язано зникнення кодів з вихідної послідовності – з явищем "биття" чи блокуванням цих кодів досліджуваним АЦП. Для того, щоб уникнути "биття" при дослідженнях на періодичному сигналі використовують стохастичну дискретизацію. Проте реалізація генераторів з контрольованим законом розподілу моментів дискретизації не дозволяє тестувати прецизійні перетворювачі.

В робочому діапазоні АЦП крок квантування дорівнює $q_0 = 1/2^n$, де n - розрядність АЦП. Інтервалу q_0 відповідає проміжок часу:

$$t_{q_0} = \frac{q_0}{\upsilon}. \tag{6}$$

Середнє значення t_{q_0} за усіма крутостями можна знайти, усереднюючи (6) по всьому діапазону зміни випадкової величини υ з вагою, що дорівнює густині розподілу $p(\upsilon)$. Значення виразу (6) не залежить від номеру підінтервалу квантування, тому усереднене значення не буде залежати від нього. Отже, для всіх підінтервалів квантування середній час, за який проходить стробування даного інтервалу, однаковий. Тому при відсутності стробоскопічного явища биття, густина розподілу продискретизованих значень вхідного сигналу буде рівномірною.

Для аналізу ефекту биття представимо тривалість будь-якої крутості у вигляді

$$T = n\Delta t + t_\varphi, \;\; n = i_{\min}, \; i_{\min}+1, ..., i_{\max}-1, \tag{7}$$

де $i_{\min}, i_{\max}$ - деякі цілі числа, причому $i_{\min} < i_{\max}$.

Вираз (7) за формою запису аналогічний виразу для операції квантування значення T квантувачем з шириною кванту Δt. У такому випадку t_φ можна трактувати як похибку квантування. Нехай $T_{\min} = i_{\min}\Delta t$, $T_{\max} = i_{\max}\Delta t$. Тоді, якщо вибирати $T_{\min}$, $T_{\max}$ кратними величині Δt, похибка квантування при таких умовах буде рівномірною. Оскільки завжди можна обирати $T_{\min}$ і $T_{\max}$ таким чином, щоб вони задовольняли вищевказаній умові, то рівномірний закон розподілу крутостей ідеально підходить зі статистичної точки зору для формування сигналу випробування. Отже, ПТІВТ не створює ефекту “биття” у вихідній послідовності АЦП.

Визначення ХП АЦП на базі ПТІВТ

На базі запропонованого тестового сигналу найпростіше можна реалізовувати статистичну методологію оброблення відліків АЦП. Цей підхід добре вивчений і використовується для періодичних гармонічних та лінійних сигналів. Проте використання спектрально бідних періодичних сигналів робить цей метод некоректним.

По-перше, він не адекватний реальним умовам експлуатації, в яких АЦП функціонує з широкосмуговими сигналами. Послідовне випробування на гармонічних сигналах змінної частоти не виправляє положення, оскільки через нелінійність АЦП безпосереднє застосування принципу суперпозиції є неправомірним.

По-друге при використанні періодичних випробувальних сигналів важко уникнути стробоскопічного ефекту “биття”, пов’язаного з кратністю частоти вхідного сигналу та частоти дискретизації.

Згідно статистичного методу будується гістограма вихідних кодів АЦП. Цифровий сигнал досліджуваного АЦП реєструється $M \cdot 2^n$ разів і підраховується число випадань M_j кожного $j = 0,1,....,2^n - 1$-го коду досліджуваного АЦП.

Диференціальна нелінійність визначається наступним чином:

$$\delta_{LD} = \frac{U_D}{2^n}(M_j - M), \tag{8}$$

де U_D - динамічний діапазон перетворювача.

Зменшуючи значення δ (і враховуючи тим самим M), можно зробити похибку визначення диференціальної нелінійності надзвичайно низькою.

Значення неперервного випробувального сигналу перетворюється n-розрядним АЦП у дискретну множину кодових комбінацій $(0,1,....,2^n - 1)$ точки переходу з j-ої кодової комбінації на (j+1)-у. Тоді характеристика “вхід-вихід” АЦП однозначно описується впорядкованим набором пар $(\tilde{u}_0,0),(\tilde{u}_1,1).....(\tilde{u}_{2^n-1},2^n-1)$, тому що при зміні вхідного сигналу в інтервалі $[\tilde{u}_j, \tilde{u}_{j+1})$ зберігається j-та кодова комбінація на виході АЦП.

В результаті дослідження АЦП методом накопичення відліків отримується деякий розподіл частот появи кодових комбінацій. Частота випадання будь-якого j-го коду дорівнює $M_j/(M\cdot 2^n)$. Звідки на основі (4) і (8), отримується:

$$\widetilde{U}_i = \frac{U_D}{M\cdot 2^n}\sum_{j=0}^{i} M_j,\ i=0,...,2^n-1. \qquad (9)$$

Використовуючи оцінки рівнів квантування, можна побудувати ХП АЦП. Метод статистичного накопичення з використанням ПВС для вимірювання ХП АЦП дозволяє адекватно оцінити ширину кванта досліджуваного АЦП, але враховуючи, що при цьому про перетворений сигнал лише апріорно відомо густину розподілу амплітудних значень, то неможливо визначити деякі параметри АЦП, такі, наприклад, як немонотонність ХП досліжуваних АЦП. Для виявлення подібного ефекту необхідно мати однозначний зв'язок між амплітудними значеннями сигналів на вході АЦП і його виході, а для цього потрібно відновлювати форму вхідного сигналу.

При відомій формі імпульсу та моментів часу перемикання сигналу при досягненні меж діапазону, встановлення взаємно однозначної відповідності між аналоговими значеннями сигналу та квантованими значеннями сигналу не є складною задачею. Це потребує лише однократної синхронізації з послідовністю відліків АЦП, тобто визначення однієї точки аналогового сигналу, що відповідає будь-якому відліку. Після цього на відомій частоті стробування АЦП і формул, що описують форму імпульсів, можна визначити послідовність $\{x_j\}_j = 1,...,N$ значень аналогового сигналу, пов'язану з отриманою в експерименті послідовністю значень $\{y_j\}_j = 1,...,N$ вихідного сигналу АЦП, де $x_j = x(j\Delta t)$, $y_j = y(j\Delta t)$, а Δt - період стробування АЦП.

Найбільш складним обмеженням, що накладає жорсткі вимоги до формування сигналу випробування є припущення про миттєве перемикання з однієї крутості на іншу. Існує кінцевий час x_i перемикання крутостей, причому, x_i через наявність багатьох чинників доцільно трактувати як випадкову величину, корельовану з крутостями сусідніх імпульсів. Отже, апріорних параметрів недостатньо і необхідно приймати додаткові заходи для усунення невизначеності, пов'язанної з відсутністю чіткого контролю величин x_i. Встановлення однозначної відповідності між значеннями аналогового сигналу та вхідного сигналу АЦП може бути досягнуто лише синхронізацією з аналоговим сигналом на кожній крутості, тобто визначенням початкової фази чи інтервалу часу від першого перетворення на даній крутості за перетвореним АЦП значенням вхідного сигналу.

Розглянутий метод дозволяє повністю відновити вхідний сигнал і використати його для вимірювання ХП АЦП за допомогою методик, спеціально розроблених для детермінованих сигналів, але функціонувати при цьому зі спектрально багатим сигналом випробування.

Аналіз продуктивності методу визначення ХП АЦП

Оцінювання продуктивності запропонованого методу проводиться шляхом аналізу числа операцій, необхідних для оброблення масивів послідовностей $\{x_j\}$ і $\{y_j\}$, які є основою реалізації методу визначення ХП АЦП. Для статистичного методу на базі ПТІВТ використовувася модифікований метод сортування даних [5]. Класичний метод є одним з методів внутрішнього сортування. Модифікація методу сортування використовує наявність масива відліків АЦП $\{y_j\}_{j=1,...n}$ і базується на проведені попереднього оброблення даних.

Нехай досліджується n-розрядний АЦП. Відомі його теоретичні 2^n кодових комбінацій. Для наглядності нехай вони знаходяться в деякому масиві $\{y_j^T\}$. Оцінюється число операцій порівняння, які потрібно в середньому для реалізації цієї процедури. Для отримання достовірних оцінок проводилось накопичення на кожну кодову комбінацію в середньому Q відліків, де Q залежить від прийнятого рівня достовірності, тобто $M_{CM} = Q\cdot 2^n$.

Для першої кодової комбінації необхідно зробити M_{CM} порівнянь, для другої в середньому $(M_{CM}-1)$ порівнянь, для третьої в середньому $(M_{CM}-2Q)$,..., для передостанньої кодової комбінації – в середньому $2Q$ порівнянь.

Загальне число порівнянь дорівнює сумі арифметичної прогресії:

$$C_1 = 0{,}5(M_{CM}+2Q)(2^n-1). \tag{10}$$

В результаті даної процедури отримується частково впорядкована послідовність $\{x_i\}$ і повністю впорядкована послідовність $\{y_i\}$. Часткова впорядкованість тут означає, що аналогові значення, що відповідають одній і тій же кодовій комбінації не будуть упорядковані між собою.

Після попереднього сортування запускається метод класичного сортування. Зважаючи на те, що було проведено попереднє сортування, перестановки елементів $\{x_i\}$ будуть проводитись в середині групи, відповідної кодової комбінації.

Для виконання цієї процедури у випадку немонотонної характеристики перетворення при рівні немонотонності $\pm$ 3 ОМР оцінкою знизу числа операцій буде:

$$C_2 = 0{,}5(2M_{CM}-Q)Q. \tag{11}$$

Користуючись цими виразами можна отримати формулу для обчислення загального числа операцій для реалізації запропонованого методу у випадку модифікованого методу сортування даних

$$C_{CM} = C_1 + C_2 = 0{,}5(M_{CM}+2Q)(2^n-1) + 0{,}5(2M_{CM}-3Q)3Q. \tag{12}$$

Оцінювання продуктивності запропонованого методу виконаємо шляхом порівняння його з гістограмним методом визначення ХП на базі синусоїдального тестового сигналу. Для даного методу загальне число операцій дорівнює [4]:

$$C_{GM} = 0{,}5(M_{GM}+1)(M_{GM}-1). \tag{13}$$

Для оцінювання якості методу пропонується використовувати критерій ефективності, що характеризує виграш у продуктивності:

$$G = \frac{C_{GM}}{C_{CM}}. \tag{14}$$

Необхідний обсяг вибірки для гістограмного методу оцінюється так. Середнє число відліків найменш імовірних кодів (середніх у графіку розподілу) для синусоїди визначається з похибкою, що не перевищує 0,1 ОМР. Для такої похибки обсяг вибірки дорівнює [4]

$$M_{GM} = 50\pi \cdot 2^n. \tag{15}$$

Підставивши (15) і (13) у вираз (14) можна отримати значення коефіцієнта продуктивності. На рисунку 1 представлено залежність продуктивності статистичного методу визначення ХП від розрядності досліджуваних АЦП.

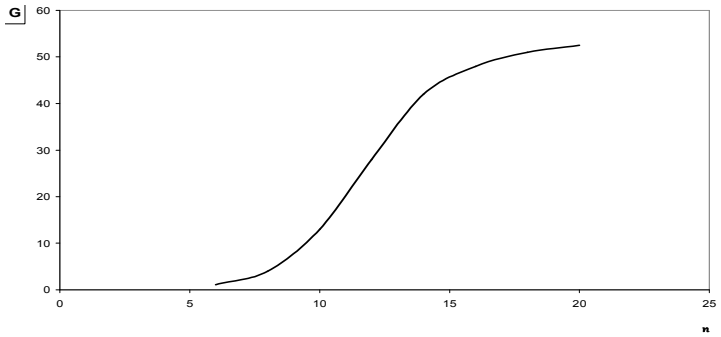


Рисунок 1 – Залежність продуктивності методу від розрядності АЦП

Як видно з графіка даний метод характеризується високими показниками продуктивності особливо для АЦП великої розрядності. Також необхідно підкреслити експресивний характер розглянутого методу. Оцінювання функції “вхід-вихід” проводиться одночасно у всій смузі досліджуваного АЦП.

Висновки

1. В результаті проведеного аналізу різних тестових сигналів, особливості яких впливають на ефективність визначення ХП АЦП, як тестовий запропоновано послідовність трикутних імпульсів з випадковою тривалістю. Виконано дослідження спектральних і статистичних властивостей ПТІВТ з лінійною формою імпульсу з метою його можливого використання як випробувального сигналу при визначенні ХП АЦП. Показано, що даний сигнал має переваги у порівнянні з іншими тестовими сигналами при динамічних вимірюваннях ХП АЦП, в плані забезпечення адекватності умов вимірювання умовам його реально експлуатації. Доведено, що при рівномірній дискретизації даного тестового сигналу відсутні "биття" у вихідній послідовності АЦП.

2. Запропонований метод дослідження АЦП дозволяє діагностувати немонотонність ХП АЦП в динамічному режимі функціонування, а також визначати диференціальну нелінійність перетворювача. Адекватність визначення ХП АЦП обумовлена можливістю моделювання різних динамічних режимів та однаковою контрольованою достовірністю для всіх її дискретних значень. Це забезпечується завдяки гнучкій керованості форми енергетичного спектра випробувального сигналу у заданій смузі частот та рівномірності розподілу значень тактового сигналу в робочому діапазоні.

4. Виконано оцінювання продуктивності запропонованого методу. У порівнянні з гістограмним методом на базі синусоїдального сигналу запропонований метод характеризується виграшем у продуктивності в 1,5 … 48 разів залежно від розрядності досліджуваного АЦП. З урахуванням того, що при контролі на гармонічному сигналі необхідно знімати гістограму розподілу кодів на кількох частотах, а також, враховуючи те, що для розрахунку ХП при використанні гармонічного сигналу потрібні складніші обчислення, можна стверджувати, що запропонований метод дозволяє отримати виграш у часі ще на порядок вищий, при одночасному забезпеченні умов вимірювання, адекватних реальним умовам експлуатації АЦП.

Список літератури

1. Брагин А. Л. Основы метрологического обеспечения аналого-цифровых преобразователей электрических сигналов/ А. А. Брагин, А. Л. Семенюк. – М.: Издательство стандартов, 1989. – 164с.

2. Гельман М. М. Системные аналого-цифровые преобразователи и процессоры сигналов/ М.М Гельман. – М.: Мир, 1999. – 559 с.

3. Грановский В. А. Динамические измерения / В. А. Грановский – Ленинград: Энергоатомиздат. – 1984. – 224с.

4. Руднев П.И. Динамические параметры аналого-цифровых преобразователей и методы их измерений/ П.И.Руднев, Б.А.Хаджи, В.Ю.Чернышев// Радиотехника и электроника. – 1993. – № 10. – С.1968-1876.

5. Загурский В. Я. Использование статистического метода контроля аналого-цифровых преобразователей для расчета динамических погрешностей / В. Я. Загурский, Н.Я. Семенова // Автоматика и вычислительная техника. – 1992. – № 6. – С. 38 – 44.

Відомості про авторів

Кичак Василь Мартитнович – д.т.н., професор, зав.кафедрою телекомунікаційних систем і телебачення, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 46-66-65.

Бортник Сергій Геннадійович – аспірант кафедри телекомунікаційних систем і телебачення, Вінницький національний технічний університет, Хмельницьке шосе, 95, м.Вінниця, 21021, тел.59-86-74, sbortnyk@gmail.com

Пунченко Наталія Олегівна – аспірант кафедри телекомунікаційних систем і телебачення, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

УДК 621.396.6

Л.Б. ЛІЩИНСЬКА

Вінницький національний технічний університет, м. Вінниця

ОЦІНКА ОСНОВНИХ ПАРАМЕТРІВ ІМІТАНСНИХ ЛОГІЧНИХ ЕЛЕМЕНТІВ

Анотація. Проведено обґрунтування основних параметрів імітансних логічних елементів: швидкодії, коефіцієнту об‘єднання по входу, коефіцієнту розгалуження, коефіцієнту стійкості, споживаної потужності і потужності, яка витрачається на переключення. Отримані аналітичні вирази для цих параметрів, які придатні до використання при реалізації імітансних ЛЕ як на біполярних, так і польових транзисторних структурах.

Ключові слова: імітанс, узагальнений перетворювач імітансу, імітансний логічний елемент.

Аннотация. Проведено обоснование основных параметров иммитансных логических элементов: быстродействия, коэффициента объединения по входу, коэффициента разветвления, коэффициента устойчивости, потребляемой мощности и мощности, которая затрачивается на переключение. Получены аналитические выражения для этих параметров, которые могут быть использованы при реализации иммитансных ЛЭ как на биполярной, так и полевой транзисторных структурах.

Ключевые слова: иммитанс, обобщенный преобразователь иммитанса, иммитансный логический элемент.

Abstract. The ground of basic parameters of immittance logical elements is conducted: fast-acting, coefficient of association on an entrance, coefficient of fork, coefficient of firmness, watts-in and power which is expended on switching. Analytical expressions are got for these parameters, what can be used for realization of immittance LE both on bipolar and to the field transistor structures.

Keywords: immittance, generalized transformer of immittance, immittance logical element.

Вступ

В обчислювальній та інформаційній техніці широке застосування отримали відеоімпульсні логічні елементи (ЛЕ) [1]. У телекомунікаційних системах знаходять застосування радіочастотні ЛЕ [2]. У системах обробки зображень – оптоелектронні ЛЕ [3]. Найважливішим параметром таких ЛЕ є швидкодія, визначувана часом переходу з одного логічного рівня на інший. Враховуючи, що робота всіх вищерозглянутих ЛЕ базується на використанні нелінійних властивостей транзисторів, їх швидкодія практично знаходиться на рівні швидкодії відеоімпульсних ЛЕ. Крім того, відеоімпульсні та оптоелектронні ЛЕ у процесі роботи вимагають комутації великих значень струму (декілька мА), що, зі зростанням ступеня інтеграції, призводить до проблеми тепловідведення. Покращення цих параметрів є актуальною проблемою сучасної цифрової електроніки.

Частково вона може бути вирішена шляхом використання імітансних ЛЕ [4], що використовують принцип нечіткого імітансу [5] і працюючих у діапазоні НВЧ, коли у процесі роботи транзистор знаходиться тільки в активному режимі, а потужність інформаційного сигналу не перевищує 10^{-5} Вт [6].

Мета роботи

Найважливішими параметрами імітансних ЛЕ, окрім швидкодії, є: коефіцієнт об'єднання по входу $K_{об}$; коефіцієнт розгалуження по виходу $K_{роз}$; споживана потужність. Враховуючи, що у даний час відсутня інформація про перераховані параметри імітансних ЛЕ, метою роботи є їх аналітичне обґрунтування і кількісна оцінка.

Аналітичне обґрунтування

В основі роботи будь-якого імітансного ЛЕ лежить узагальнений перетворювач імітансу (УПІ), до входу якого одночасно, послідовно або довільно, підключаються перетворювані імітанси W_{Γ_i}, які є вихідними імітансами $W_{вих.i}$ інших імітансних ЛЕ, підключених до входу ЛЕ, що розглядається (рис. 1).

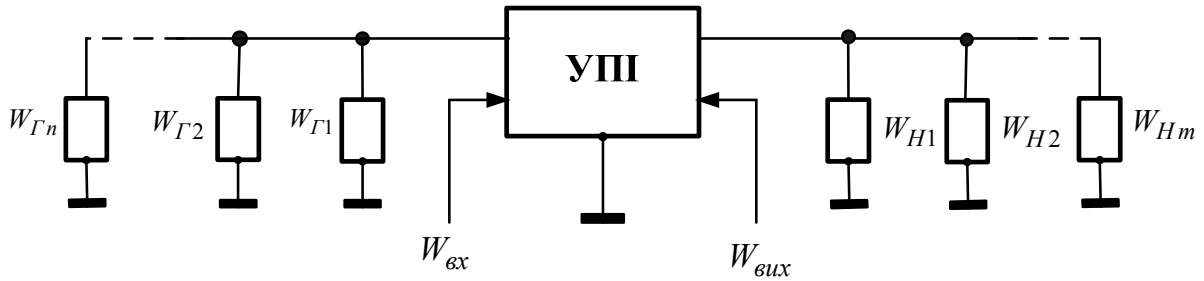


Рисунок 1 – Узагальнена схема імітансного логічного елемента

До його виходу підключені імітанси навантаження W_{H_i}, які дорівнюють вхідним імітансам $W_{вх.i}$ ЛЕ, підключених до виходу ЛЕ, що розглядається. У якості УПІ таких ЛЕ отримали застосування біполярні та уніполярні напівпровідникові структури, що здатні працювати на частотах до *100 ГГц* і вище [7]. Виходячи з цього, проведемо оцінку швидкодії імітансного ЛЕ, що реалізовується на біполярному і

польовому транзисторах. Вважатимемо, що до входу УПІ підключений лише один перетворюваний імітанс W_{Γ_i}, а до його виходу підключено лише одне навантаження W_{H_i}.

Швидкодію імітансного ЛЕ визначатимемо часом τ, протягом якого відбудеться стабілізація значення вихідного перетвореного імітансу $W_{вих}$ від моменту появи (підключення) до входу УПІ перетворюваного імітансу W_{Γ_i}. Цей час буде визначатися постійною часу $\tau_{вх}$ вхідного ланцюгу УПІ, часом затримки сигналу в УПІ $\tau_{УПІ}$ і постійною часу $\tau_{вих}$ вихідного ланцюга УПІ:

$$\tau = \tau_{вх} + \tau_{УПІ} + \tau_{вих}.$$

Постійні часу $\tau_{вх}$ і $\tau_{вих}$ залежать від величини і значення вхідного $W_{вх}$ і вихідного $W_{вих}$ імітансів, а також параметрів ланцюгів, підключених до входу і виходу УПІ W_{Γ_i} і W_{H_i}. Переходячи до термінів провідності знаходимо:

– при $\mathrm{Im}\left(Y_{\Gamma_1} + Y_{вх}\right) < 0$ і $\mathrm{Im}\left(Y_{H1} + Y_{вих}\right) < 0$:

$$\tau_{вх.L} = \frac{\mathrm{Im}\left(Y_{\Gamma 1} + Y_{вх}\right)}{\omega \mathrm{Re}\left(Y_{\Gamma 1} + Y_{вх}\right)};\ \tau_{вих.L} = \frac{\mathrm{Im}\left(Y_{H1} + Y_{вих}\right)}{\omega \mathrm{Re}\left(Y_{H1} + Y_{вих}\right)}; \quad (1)$$

– при $\mathrm{Im}\left(Y_{\Gamma 1} + Y_{вх}\right) > 0$ і $\mathrm{Im}\left(Y_{H1} + Y_{вих}\right) > 0$:

$$\tau_{вх.C} = \frac{\mathrm{Re}\left(Y_{\Gamma 1} + Y_{вх}\right)}{\omega \mathrm{Im}\left(Y_{\Gamma 1} + Y_{вх}\right)};\ \tau_{вих.C} = \frac{\mathrm{Re}\left(Y_{H1} + Y_{вих}\right)}{\omega \mathrm{Im}\left(Y_{H1} + Y_{вих}\right)}. \quad (2)$$

У разі реалізації УПІ на основі біполярної транзисторної структури часова затримка сигналу визначається сумою часу всіх затримок розповсюдження сигналу у ній [8]:

$$\tau_{УПІ.Б} = \tau_E + \tau_K + \tau_Б + \tau_Z + \tau_B,$$

де τ_E – час заряду ємкості переходу емітер–база; τ_K – постійна часу колекторного переходу; $\tau_Б$ – час перенесення носіїв через базу; τ_Z – час перенесення носіїв через область об'ємного заряду колекторного переходу; τ_B – час заряду ємкості переходу колектор–підкладка.

Ця сумарна затримка може бути розрахована за результатами вимірювання граничної $f_{гр}$ або максимальної частоти генерації $f_{\max}$ біполярного транзистора, а також максимально–досяжного коефіцієнту стійкого підсилення транзистора $K_{ms.k}$ у схемі зі спільним колектором

$$\tau_{УПІ.Б} = \frac{1}{2\pi f_{гр}} = \frac{1}{r_б C_K \left(2\pi f_{\max}\right)^2} = \frac{1}{2\pi f_{вим} K_{ms.k}}, \quad (3)$$

де $r_б$ і C_K – омічний опір бази і ємкість колекторного переходу.

У разі реалізації УПІ на основі польового транзистора з урахуванням того, що значення паразитних параметрів транзистора враховуються при розрахунку $\tau_{вх}$ і $\tau_{вих}$ у провідності $Y_{\Gamma 1}$ і Y_{H1}, час затримки сигналу $\tau_{УПІ.П}$ у ньому, при розгляді каналу транзистора як передавальній лінії без втрат і частотною залежністю крутизни ВАХ транзистора у вигляді [9]

$$S_T = S_o \ell^{j\omega\tau} \Big/ \left(1 + j\omega R_i C_{ЗВ}\right), \quad (4)$$

буде дорівнювати

$$\tau_{УПП.П} = \omega^{-1} arctg\left(\operatorname{Im} S_T / \operatorname{Re} S_T\right) = \tau + \omega^{-1} arctg\Omega_S, \quad (5)$$

де S_o – низькочастотне значення крутості; τ – час прольоту каналу носіями струму; R_i і $C_{ЗВ}$ – диференціальний опір та ємкість між затвором і витоком транзистора., $\Omega_S = \omega_S / \omega$, ω_S – гранична частота ПТ за крутизною.

У першому наближенні величина τ залежить від довжини каналів ℓ польового транзистора і дрейфової швидкості $\upsilon_{\partial p}$ носія струму у ній $\tau \approx \ell / \upsilon_{\partial p}$.

Коефіцієнт об'єднання по входу $K_{об}$ імітансного ЛЕ розрахуємо у припущенні, що ЛЕ, які підключаються до його входу, є ідентичними і мають вихідний імітанс $W_{Г1}$. Враховуючи, що імітансні ЛЕ найбільш ефективні у діапазоні НВЧ, де, з точки зору стійкості, доцільне використання заземлених схем, розрахуємо величину $K_{об}$ у припущенні, що до входу УПІ підключено *n* ідентичних заземлених ЛЕ з вихідною провідністю $Y_{Г1}$ Тоді сумарна перетворювана провідність буде дорівнювати $Y_Г = nY_{Г1}$. Подальший розрахунок залежить від характеру інформаційного параметра. Наприклад, розглянемо *LC*–імітансний ЛЕ, коли у якості інформаційного параметру використовується індуктивний та ємкісний імітанс. У загальному випадку, для реального УПІ залежність складових перетвореної провідності $Y_{вих}$ від перетворюваної $Y_Г$ є нелінійною та обмеженою $\operatorname{Im} W_{Г.\min}$ і $\operatorname{Im} W_{Г.\max}$ (рис. 2).

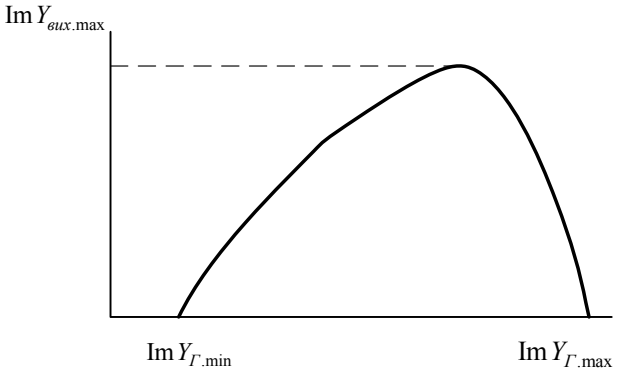


Рисунок 2 – Гіпотетична залежність уявної складової $\operatorname{Im} Y_{вих}$ перетвореної провідності УПІ від уявної складової $\operatorname{Im} Y_Г$ перетворюваної провідності

Виходячи з принципу функціонування імітансного ЛЕ умовою його роботи є $0 < \operatorname{Im} Y_{вих} < \operatorname{Im} Y_{вих.\max}$ при $\operatorname{Im} W_{Г.\min} < \operatorname{Im} W_Г < \operatorname{Im} W_{Г.\max}$. Виходячи з цього, враховуючи технологічний, режимний і температурний розкид перетворюваної провідності $\Delta \operatorname{Im} W_Г$, знаходимо

$$K_{об} = \frac{\operatorname{Im}\left(Y_{Г.\max} - \operatorname{Im} Y_{Г.\min}\right)}{\Delta \operatorname{Im} W_Г}. \quad (6)$$

При розрахунку $K_{об}$ величина $\Delta \operatorname{Im} W_Г$ також враховує умови завадостійкості.

Оцінку коефіцієнта розгалуження по виходу $K_{роз}$ також проведемо у припущенні, що ЛЕ, які підключаються до виходу імітансного ЛЕ, є ідентичними. Тому, виходячи з рис. 2, величина уявної складової $\operatorname{Im} Y_{вих}$ перетвореної провідності повинна бути у діапазоні від $\operatorname{Im} Y_{Г.\max}$ до $\operatorname{Im} Y_{Г.\min}$. При цьому, коефіцієнт розгалуження $K_{роз}$ залежить, перш за все, від потужності вихідного сигналу $P_{вих}$ і чутливості ЛЕ, які підключаються до виходу ЛЕ. Під чутливістю ЛЕ розумітимемо мінімальну потужність сигналу $P_{вх.\min}$ на його вході, яка розвиває на його виході стандартну потужність $P_{вих.\max}$ при

заданому співвідношенні сигнал/шум. Стандартною потужністю $P_{вих.\max}$ вважаємо максимальне значення вихідної потужності ЛЕ, при якій забезпечується квазілінійний режим роботи ЛЕ, що підключається до його виходу. Мінімальна потужність сигналу на вході ЛЕ $P_{вх.\min}$ повинна перевищувати потужність власних шумів ЛЕ $P_{ш.власн}$, приведених до входу ЛЕ, що визначає його коефіцієнт шуму [10]

$$K_ш = 1 + \frac{P_{ш.власн.11}}{\kappa T_o П_ш q_{вх}}, \tag{7}$$

де κ – постійна Больцмана, $T_o = 293\kappa$, $П_ш$ – шумова смуга, $q_{вх}$ – коефіцієнт розузгодження вхідного ланцюга.

Використовуючи (7), знаходимо

$$P_{вх.\min} \succ P_{ш.власн.11} = \kappa T_o П_ш q_{вх}(K_ш - 1). \tag{8}$$

З урахуванням (8), коефіцієнт розгалуження імітансного ЛЕ буде дорівнювати

$$K_{роз} = \frac{P_{вих.\max}}{P_{вх.\min}} < \frac{P_{вих.\max}}{\kappa T_o П_ш q_{вх}(K_ш - 1)}. \tag{9}$$

Аналіз (9) показує, що основними шляхами збільшення цього коефіцієнта є зменшення шумової смуги частот $П_ш$ і коефіцієнта шуму $K_ш$ УПІ.

Враховуючи, що УПІ реалізується на основі потенційно–нестійких транзисторних структур, його найважливішим параметром є також запас стійкості. Для кількісної оцінки запасу стійкості ЛЕ можливе використання інваріантного коефіцієнта стійкості K_c, який визначається через імітансні *W*-параметри УПІ та імітанси генератора $W_Г$ (перетворюваний імітанс) і навантаження W_H [11]

$$K_C = \frac{2\,\mathrm{Re}(W_{11} + W_Г)\,\mathrm{Re}(W_{22} + W_H) - \mathrm{Re}(W_{12}W_{21})}{|W_{12}W_{21}|}. \tag{10}$$

Для забезпечення абсолютної стійкості ЛЕ необхідно, щоб значення $K_C > 1,$ яке забезпечується за рахунок збільшення $\mathrm{Re}W_Г$ або $\mathrm{Re}W_H$.

Величина споживаної потужності ЛЕ визначається двома складовими: постійною P_o , яка є незмінною і визначається положенням робочої точки транзистора, і високочастотною *P*, значення якої є у межах від $P_{вх.\min}$ до $P_{вих.\max}$. Для ефективної роботи УПІ робоча точка транзистора повинна знаходиться в активній області, де коефіцієнт передачі по струму (або крутизна) є максимальним. Для малосигнального біполярного транзистора цей режим забезпечується при струмі колектора порядку (2–3 мА) і напругою E_K=5B, тобто $P_o = (10-15)$ мВт Для квазілінійного режиму роботи $P_{вих.\max} \le 10^{-4}$Вт , що значно менше P_o . Таким чином, за споживаною потужністю імітансні ЛЕ знаходиться на рівні споживання сучасних відеоімпульсних ЛЕ. Але їх особливість полягає у тому, що величина P_o не змінюється у процесі роботи ЛЕ, що виключає виникнення нелінійних перехідних процесів, а потужність сигналу, яка витрачається на переведення ЛЕ з одного логічного стану в інше, не перевищує 10^{-4}Вт.

Експериментальні результати

З метою оцінки швидкодії ЛЕ проведені дослідження перехідних процесів у схемі (рис. 3), в якій на біполярному транзисторі BFS25A, включеному за схемою зі спільним колектором, реалізований УПІ в режимі прямого перетворення індуктивного імпедансу *L2*, що періодично підключається ключем *S1*, керованим імпульсним генератором *V4*, до входу транзистора. Вихідний ланцюг навантажувався генератором гармонійного сигналу *V3* з частотою 7,5 ГГц з амплітудою напруги 10 мкВ. Реєструвався вихідний струм схеми.

Аналіз осцилограм перехідних процесів (рис.4) показує, що тривалість перехідного

процесу стабілізації фази сигналу (визначає характер реактивності) не перевищує 1/4 періоду коливань. У даному випадку маємо $\tau < 30$ пс. Враховуючи, що для даного типу транзистора $\tau_{УПП} \approx 1,6$ пс, можна зробити висновок про визначальний вплив величини перетворюваних імітансів на швидкодію імітансного ЛЕ. Більш тривалим є перехідний процес стабілізації амплітуди. Але він не визначає працездатність ЛЕ і може бути зменшений за рахунок зниження величини реактивності перетворюваного імітансу, що, у свою чергу, підвищить його швидкодію.

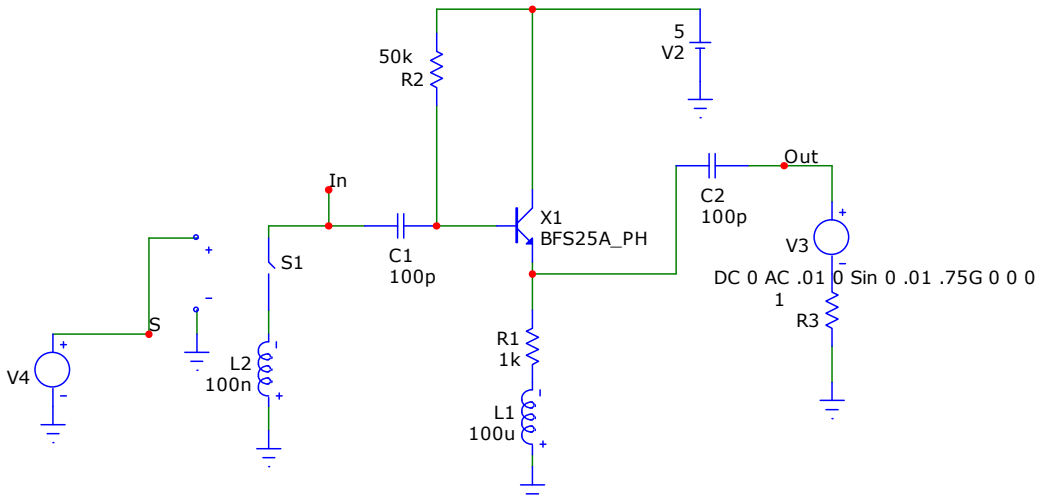


Рисунок 3 – Експериментальна схема для дослідження часових характеристик імітансного ЛЕ у режимі зворотного перетворення індуктивного імітансу (*L2*)

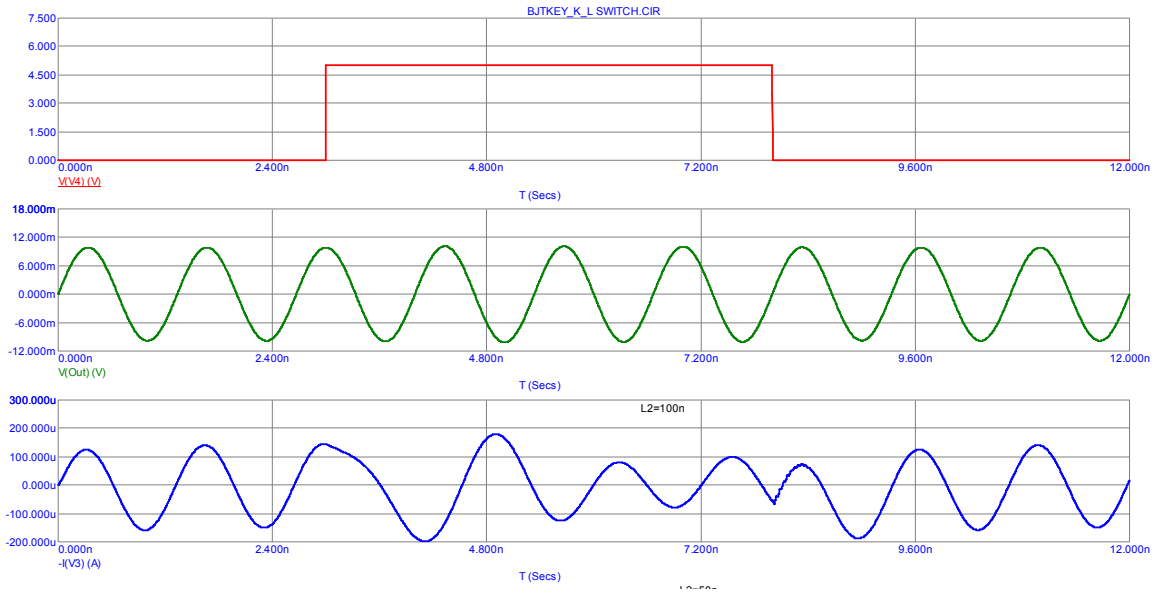


Рисунок 4 – Осцилограми перехідних процесів у схемі на рис. 3

Як наголошувалося у попередньому розділі, при проектуванні імітансних ЛЕ необхідно контролювати запас стійкості схеми. Характерним прикладом можливості порушення режиму стійкості є використання біполярного транзистора у режимі перетворення ємкісного імітансу конденсатора *C3* у вхідний імітанс схеми (рис.5).

Як випливає з осцилограм на рис. 6, при опорі задаючого генератора сигналу *V3* рівного 10 Ом, під час перехідного процесу відбувається збудження схеми, що істотно збільшує τ . Цей негативний ефект легко ліквідується за рахунок збільшення *R3* до 100 Ом, що, як випливає з (10), призведе до зростання K_c . Крім того, існує ще два шляхи подолання цього явища. Це вибір робочої частоти або величини перетворюваного імітансу, при яких дійсна складова перетвореного імітансу $\mathrm{Re}\, W_{вих}$ залишається позитивною у всіх діапазонах роботи.

Виходячи з (6), коефіцієнт об'єднання по входу імітансного ЛЕ залежить від величини перетворюваного імітансу W_Γ, що визначає перетворений імітанс [9]

$$W_{вих} = W_{22} - \frac{W_{12}W_{21}}{W_{11} + W_\Gamma}, \tag{11}$$

де W_{11}, W_{22}, W_{12}, W_{21} – параметри імітансної матриці УПІ.

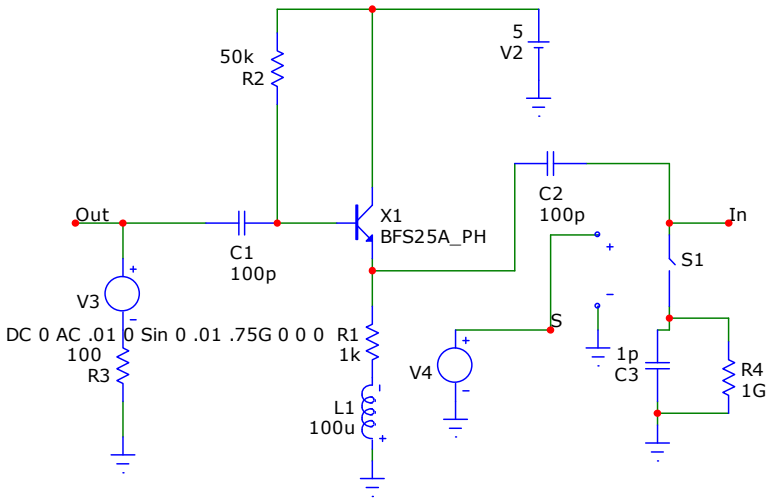
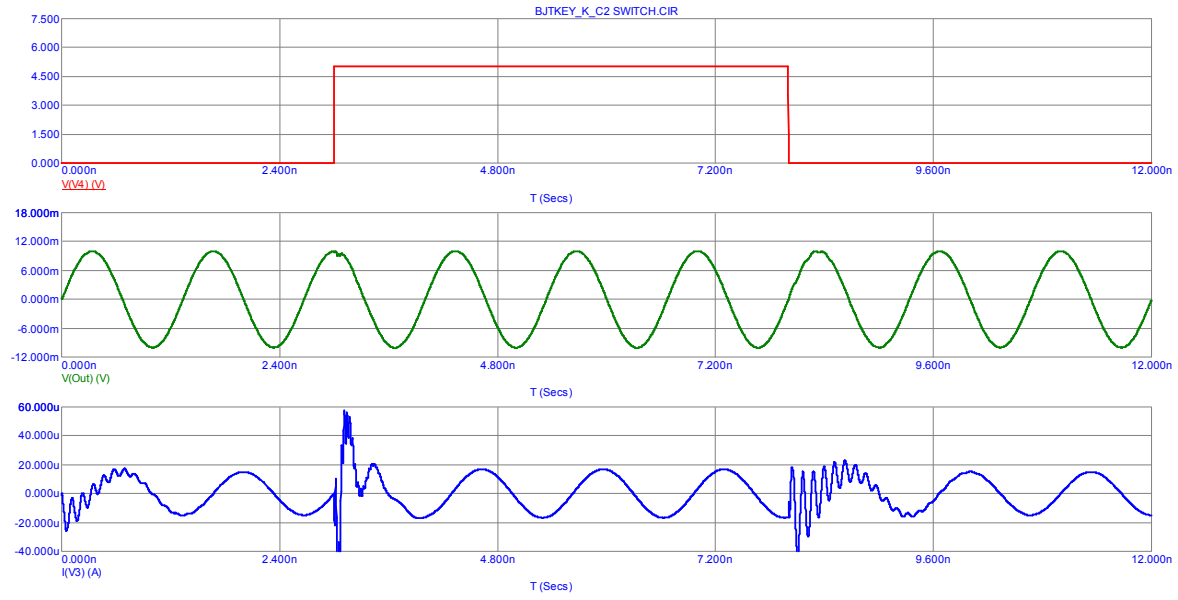
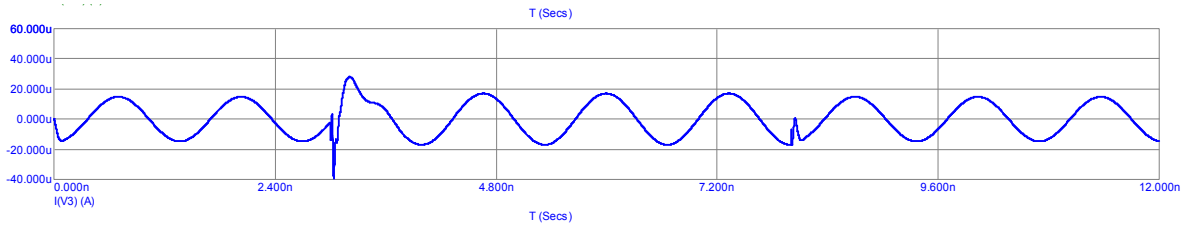


Рисунок 5 – Експериментальна схема для дослідження часових характеристик імітансного ЛЕ у режимі прямого перетворення ємкісного імітансу (*C3*)



а)



б)

Рисунок 6 – Осцилограми перехідних процесів у схемі на рис. 5 при $R3 = 10$ Ом (а) і $R3 = 100$ Ом (б)

Перетворивши (11), знаходимо

$$W_{\Gamma} = -W_{11} + \frac{W_{12}W_{21}}{W_{22} - W_{вих}}. \tag{12}$$

Враховуючи, що у загальному випадку W-параметри УПІ є комплексними, з (8) знаходимо дійсну $\mathrm{Re}\,W_{вих}$ і уявну $\mathrm{Im}\,W_{вих}$ складові перетвореного імітансу в залежності від нормованого значення σ_{Γ} перетворюваного імітансу:

$$\mathrm{Re}\,W_{вих} = \mathrm{Re}\,W_{22} - \frac{\mathrm{Re}\left(W_{12}W_{21}\right) + \sigma_{\Gamma}\,\mathrm{Im}\left(W_{12}W_{21}\right)}{\left(1+\sigma_{\Gamma}^2\right)\mathrm{Re}\left(W_{11}+W_{\Gamma}\right)}; \tag{13}$$

$$\mathrm{Im}\,W_{вих} = \mathrm{Im}\,W_{22} - \frac{\mathrm{Im}\left(W_{12}W_{21}\right) - \sigma_{\Gamma}\,\mathrm{Re}\left(W_{12}W_{21}\right)}{\left(1+\sigma_{\Gamma}^2\right)\mathrm{Re}\left(W_{11}+W_{\Gamma}\right)}, \tag{14}$$

де $\sigma_{\Gamma} = \mathrm{Im}\left(W_{\Gamma}+W_{11}\right)/\mathrm{Re}\left(W_{\Gamma}+W_{11}\right)$.

Вирази (13) і (14) є базовими при розрахунку коефіцієнта об'єднання по входу імітансного ЛЕ будь-якого виду. Наприклад, для *LC*-імітансного ЛЕ, на підставі (14), отримуємо рівняння, рішення якого визначають максимальне $\mathrm{Im}\,W_{\Gamma.\max}$ і мінімальне $\mathrm{Im}\,W_{\Gamma.\min}$ значення перетворюваного імітансу при $\mathrm{Re}\,W_{\Gamma} = 0$.

$$\mathrm{Im}\,W_{\Gamma.\max} = \sigma_{\Gamma.\max}\,\mathrm{Re}\,W_{11} - \mathrm{Im}\,W_{11}; \tag{15}$$

$$\mathrm{Im}\,W_{\Gamma.\min} = \sigma_{\Gamma.\min}\,\mathrm{Re}\,W_{11} - \mathrm{Im}\,W_{11}, \tag{16}$$

де $\sigma_{\Gamma.\max} = \left(-b+\sqrt{b^2-4ac}\right)\Big/2a$; $\sigma_{\Gamma.\min} = \left(-b-\sqrt{b^2-4ac}\right)\Big/2a$; $a = \mathrm{Im}\,W_{22}\,\mathrm{Re}\,W_{11}$; $b = \mathrm{Re}\left(W_{12}W_{21}\right)$; $c = \mathrm{Im}\,W_{22}\,\mathrm{Re}\,W_{11} - \mathrm{Im}\left(W_{12}W_{21}\right)$.

З урахуванням технологічного і температурного розкиду параметрів компонентів гібридних мікросхем γ_T, знаходимо

$$\Delta\,\mathrm{Im}\,W_{\Gamma} = \gamma_T\,\mathrm{Im}\,W_{\Gamma.\max}. \tag{17}$$

Переходячи до термінів провідності, підставляючи (15–17) в (6), знаходимо аналітичний вираз для $K_{об}$ LC-імітансного ЛЕ в залежності від параметрів матриці провідності УПІ

$$K_{об} = \frac{\mathrm{Re}\,y_{11}\left(\sigma_{\Gamma.\max} - \sigma_{\Gamma.\min}\right)}{\gamma_T\left(\sigma_{\Gamma.\max}\,\mathrm{Re}\,y_{11} - \mathrm{Im}\,y_{11}\right)}. \tag{14}$$

Для гібридних мікросхем γ_T не перевищує 5% [8]. З урахуванням імітансних параметрів сучасних транзисторних структур у діапазоні частот (1–10) ГГц величина $K_{об} \approx (20-40)$ од.

Висновки

1. Проведено теоретичне обгрунтування основних параметрів імітансних логічних елементів, таких як швидкодія, коефіцієнт об‘єднання по входу, коефіцієнт розгалуження, коефіцієнт стійкості, споживана потужність і потужність, яка витрачається на переключення. Отримані аналітичні вирази для цих параметрів, які придатні до використання при реалізації імітансних ЛЕ як на біполярних, так і польових транзисторних структурах.

2. Показано, що при реалізації імітансних ЛЕ на біполярних транзисторах з граничною частотою рівною 10 ГГц час переключення не перевищує 0,25 періоду, що складає менше 30 пс і може бути зменшено за рахунок використання більш високочастотних транзисторів та оптимізації діапазону зміни перетворюваних імітансів.

3. Коефіцієнт об‘єднання по входу залежить від величини перетворюваного імітансу і розкиду

параметрів компонентів. При 5% розкиді величина $K_{об} \approx (20-40)$ од. Величина коефіцієнту розгалуження по виходу обмежена коефіцієнтом шуму УПІ і шумовою смугою частот.

4. Споживана потужність імітансних ЛЕ знаходиться на рівні споживання сучасних ЛЕ, але потужність, яка витрачається на переключення з одного логічного стану в інший, значно менша (менше 10^{-4} Вт).

5. На відміну від відеоімпульсних ЛЕ при проектуванні імітансних ЛЕ необхідно контролювати умови забезпечення їх стійкості, наприклад, шляхом погіршення добротності перетворюваного імітансу або навантаження для досягнення значення $K_c > 1$.

Автор висловлює подяку доц. Лазареву О.О. за плідне обговорення результатів роботи і допомогу при проведенні чисельних експериментів.

Література

1. Преснухин Л.Н. Цифрове вычислительные машины / Л.Н.Преснухин, П.В. Нестеров. – М.: Высш. Школа, 1981. – 511с.

2. Кичак В.М. Синтез частотно-імпульсних елементів цифрової техніки: монографія / В.М. Кичак. – Вінниця: УНІВЕРСУМ–Вінниця, 2005. – 266с. – ISBN 966-641-137-7.

3. Оптоэлектронная схемотехника / В.П. Кожемяко, О.Г. Натрошвили, Т.Б. Мартинюк, Л.Ш. Имнаишвили. – К.: УМК ВО, 1988. – 276с.

4. Ліщинська Л.Б. Імітансна логіка / Л.Б.Ліщинська, М.А. Філинюк // Інформаційні технології та комп'ютерна інженерія. – 2010. - № 2(18). – С. 25-31.

5. Лищинская Л.Б. Обоснование концепции «нечёткого імітанса» / Л.Б. Лищинская // Вимірювальна та обчислювальна техніка в технологічних процессах. – 2010. – №1. – С. 20–25.

6. Філинюк М.А. Елементи та пристрої автоматики на основі нелінійних властивостей динамічних негатронів: монографія / М.А. Філинюк, О.В. Войцеховська. – Вінниця: УНІВЕРСУМ–Вінниця, 2008. – 189с. – ISBN 978-966-641-250-1.

7. T. H. Lee, "From Oxymoron to Mainstream: The Evolution and Future of RF CMOS", IEEE International Workshop, RFIT-Radio-Frequency Integration Technology, pp. 1-6, Singapore, December 2007.

8. Николаев И. М. Интегральные микросхемы и основы их проектирования. / Николаев И. М., Филинюк Н. А. – М.: Радио и связь, 1992. – 424 с.

9. Філинюк М. А. Інформаційні пристрої на основі потенційно-нестійких багатоелектродних напівпровідникових структур Шотткі.: Монографія. / Філинюк М. А., Куземко О. М., Ліщинська Л. Б. – Вінниця: ВНТУ, 2009. – 274 с. – ISBN 978–966–641-332–4.

10. Музыка З. Н. Чувствительность радиоприемных устройств на полупроводниковых приборах / З. Н. Музыка. – М.: Радио и связь, 1981. – 168с.

11. Rollett J. Stability and power gain invariants of linear two–ports / J. Rollett // IRE Trans. Circuit Theory. – 1962. – Vol. CT–9, № 3. – P. 29–32.

Відомості про авторів

Ліщинська Людмила Броніславівна – к.т.н., доцент, здобувач ВНТУ, м. Вінниця, Хмельницьке шосе,95, L_Fil1@mail.ru.

УДК 004.27; 004.25; 004.382.2

Ю.С. ЯКОВЛЕВ, Е.В.ЕЛИСЕЕВА

Институт кибернетики имени В.М. Глушкова НАН Украины, Киев

О РЕАЛИЗАЦИИ РАСПРЕДЕЛЕНИЯ ПРИЛОЖЕНИЯ ДЛЯ ПАРАЛЛЕЛЬНОГО ВЫПОЛНЕНИЯ НА PIM-СИСТЕМЕ

Аннотация. Предложены эффективный алгоритм и непосредственно на языке С++ программа реализации алгоритма распределения фрагмента приложения между процессорами распределенной гетерогенной компьютерной системы типа PIM, которые в максимальной степени учитывают особенности архитектурно-структурной организации систем такого класса и тем самым обеспечивают быструю сходимость и сокращение времени реализации алгоритма распределения.
Ключевые слова: PIM- система, алгоритм распределения приложения, параллельная обработка, система команд.
Анотація. Запропоновані ефективний алгоритм і безпосередньо на мові С++ програма реалізації алгоритму розподілу фрагменту програми користувача між процесорами розподіленої гетерогенної комп'ютерної системи типу PIM, які в максимальному ступені враховують особливості архітектурно-структурної організації систем такого класу і тим самим забезпечують швидку збіжність і скорочення часу реалізації алгоритму розподілу.
Ключові слова: PIM-система, алгоритм розподілення програми користувача, паралельна обробка, система команд.
The abstract. Are offered effective algorithm and it is direct in language C ++ the program of implementation of a scheduling algorithm of applications between processors of the distributed heterogeneous computer system of type PIM, which in the maximum extent consider features of the is architectural-structural organisation of systems of PIM-system and by that provides sweeping convergence and abbreviation of a time of implementation of a scheduling algorithm.
Keywords: PIM-system, the application scheduling algorithm, parallel machining, the system of commands.

Введение

История развития средств вычислительной техники показала, что с точки зрения повышения производительности эффект использования новых архитектурно-структурных решений и новых методов распараллеливания приложений существенно превосходит эффект, который может быть получен путем применения новой элементной базы. Достижения интегральной технологии сделали возможным появление новых классов архитектур типа “Процессор-в-памяти” (PIM), которые реализованы на одном кристалле (чипе) и по сравнению с КС с классической архитектурой при одинаковых ресурсах процессоров и памяти обладают более высокими параметрами производительности при улучшенных значениях других пользовательских характеристик (габаритов, веса и др.), а также возможностями решать сложные и трудоемкие задачи, которые плохо поддаются решению или вообще не могут быть решены с помощью классических КС [1]. PIM-система по своим принципам построения имеет ряд особенностей: она образует иерархическую гетерогенную многопроцессорную среду, включающую ведущий процессор (ВП) со своей памятью и соединенные с ВП процессорные ядра (ПЯ), подключенные каждый к своему банку памяти. При этом ВП имеет развитую систему команд, широкие функциональные возможности и является более мощным, по сравнению с каждым ПЯ, который представлен в виде упрощенного процессора с сокращенной системой команд и поэтому является функционально ограниченным и менее мощным, но имеет малое время доступа к своему банку памяти.

Актуальность

Известные способы распределения приложений для PIM-систем [2, 3] основаны на упрощенной модели распределения, и соответственно процесс распределения реализуют только между хост-машиной и одним ВП. При этом в качестве основной единицы при анализе и разделении исходной программы пользователя используют операторы в цикле (применен операторный метод распределения), из-за сложности которого рассматривают только операторы внутри циклов, и обнаруживают зависимости по данным только для некоторых конструкций программы пользователя (для идеально вложенных циклов), при этом другие конструкции не рассматривают, что указывает на ограниченные функциональные возможности способов. Несмотря на эти упрощения, процесс распределения приложения является трудоемким и занимает большое количество времени, которое может существенно превышать время непосредственного решения задачи пользователя, увеличивая тем самым энергозатраты и стоимость эксплуатации системы в целом. Поэтому поиск нового решения проблемы распределения приложений, которое устранило бы недостатки известных способов распределения, является задачей актуальной.

Цель

Создать эффективный алгоритм и непосредственно на языке С++ программу реализации фрагмента алгоритма распределения приложений между процессорами распределенной гетерогенной компьютерной системы типа PIM, которые в максимальной степени учитывают особенности архитектурно-структурной организации систем такого класса и тем самым обеспечивает быструю сходимость и сокращение времени реализации алгоритма распределения.

Постановка задач

1). Исследовать существующие алгоритмы распределения приложений для PIM-систем и выполнить анализ их недостатков.

2). Исследовать существующие критерии распределения приложения и предложить новые, учитывающие особенности архитектурно-структурной организации PIM-систем.

2). Разработать алгоритм программы распределения приложений для параллельной реализации на PIM-системе с учетом особенностей архитектурно-структурной организации этого класса машин и выполнить его описание (комментарии).

3). Разработать программу реализации предложенного алгоритма распределения приложения по процессорам PIM-системы с использованием языка программирования C++.

Решение задач

В основу решения задачи по созданию алгоритма распределения приложения положена многоуровневая стратегия распределения, которая применительно к PIM-системе на одном кристалле содержит два уровня: сначала внутри чипа разделяют фрагмент алгоритма приложения на блоки и распределяют их внутри чипа по процессорам. Этот фрагмент алгоритма был приписан данному чипу на предыдущем уровне распределения (между хост-машиной и чипом), который здесь не рассматривается. Распределение приложения на программные блоки выполняют согласно модели распределения – между ВП и эквивалентным процессорным ядром (ПЯ*), параметры которого формируют следующим образом: за систему команд ПЯ* принимают систему команд одного ПЯ, так как все ПЯ на чипе одинаковые, величину емкости памяти ПЯ* принимают равной величине емкости всей памяти, подключенной ко всем ПЯ на этом чипе, а время реализации команды ПЯ* принимают равной времени реализации одного ПЯ, поделенного на количество ПЯ, входящих в состав ПЯ*, учитывая, что все ПЯ одинаковые и работают параллельно. Тем самым на этом уровне создают модель стратегии распределения программ пользователя из двух элементов (ВП и ПЯ*), что упрощает процесс распределения и не приводит к значительным ошибкам, поскольку на этом уровне выполняют проверку баланса загрузки процессоров ВП и ПЯ* и при необходимости из-за отсутствия баланса выполняют корректировку распределения. При этом в качестве основного критерия распределения каждого фрагмента программы пользователя на этом уровне (внутри одного чипа) принимают соответствие систем команд ВП и ПЯ* набору операций фрагмента алгоритма, который был приписан этому чипу при распределении всего приложения между хост-машиной и чипом.

На следующем уровне выполняют распределение программных блоков на модули между всеми ПЯ, входящими в набор ПЯ* одного чипа. При этом, так как все ПЯ в наборе ПЯ* одинаковые, то за основной критерий распределения модулей принимают рассчитанные их параметрические веса (времена их реализации) и соответствующие связи по данным. По значениям параметрических весов оценивают баланс загрузки модулями каждого ПЯ внутри чипа, и при отсутствии баланса выполняют перераспределение модулей между ПЯ, входящих в состав ПЯ*, для которых баланс не выполняется.

По окончании распределения формируют так называемые волновые фронты (ВФ), при этом в состав каждого ВФ включают программные блоки, независимые по данным и которые на PIM-системе могут быть выполнены одновременно. Последовательность выполнения ВФ определяют в соответствие с последовательностью выполнения программных блоков в исходном фрагменте алгоритма приложения согласно связности этих блоков по данным. Результаты распределения представляют в виде соответствующих пакетов (файлов), которые направляют в память соответствующих ВП и ПЯ для параллельного выполнения распределенных блоков приложения внутри чипа.

Предложенная стратегия распределения основана на следующих принципах [4]**:**

1. Принцип соответствия набора операций фрагмента (блока) алгоритма приложения набору системы команд процессора, на котором этот блок должен быть выполнен.

2. Принцип соответствия структуры алгоритма распределения иерархической структуре имеющихся ресурсов PIM-системы.

3. Принцип допустимой замены одинаковых ресурсов множества процессорных элементов, ориентированных на параллельную работу, и модулей памяти на один эквивалентный комплексный ресурс, вложенный в ПЯ*, содержащий один процессор с системой команд одного ПЯ и временем такта его работы, равный времени такта работы одного ПЯ, поделенной на k, где k – количество ПЯ на кристалле (чипе), и с емкостью памяти равной сумме емкостей памяти всех ПЯ на этом кристалле.

4. Принцип проверки и корректировки баланса загрузки процессоров по специфическим критериям, в частности – по критерию параметрического веса.

Согласно сформулированными выше стратегией и основными принципами распределения, разработан алгоритм программы распределения приложения по процессорам PIM-системы, часть которого, отражающая распределение между ВП и эквивалентным ПЯ*, а также между множеством ПЯ, входящих в состав ПЯ*, приведена на рисунке 1. Описание уровней распределения приложений более подробно изложено в [5]. Для части алгоритма, отображенной на рисунке 1, разработана программа на C++, описание блоков которой приведено ниже.

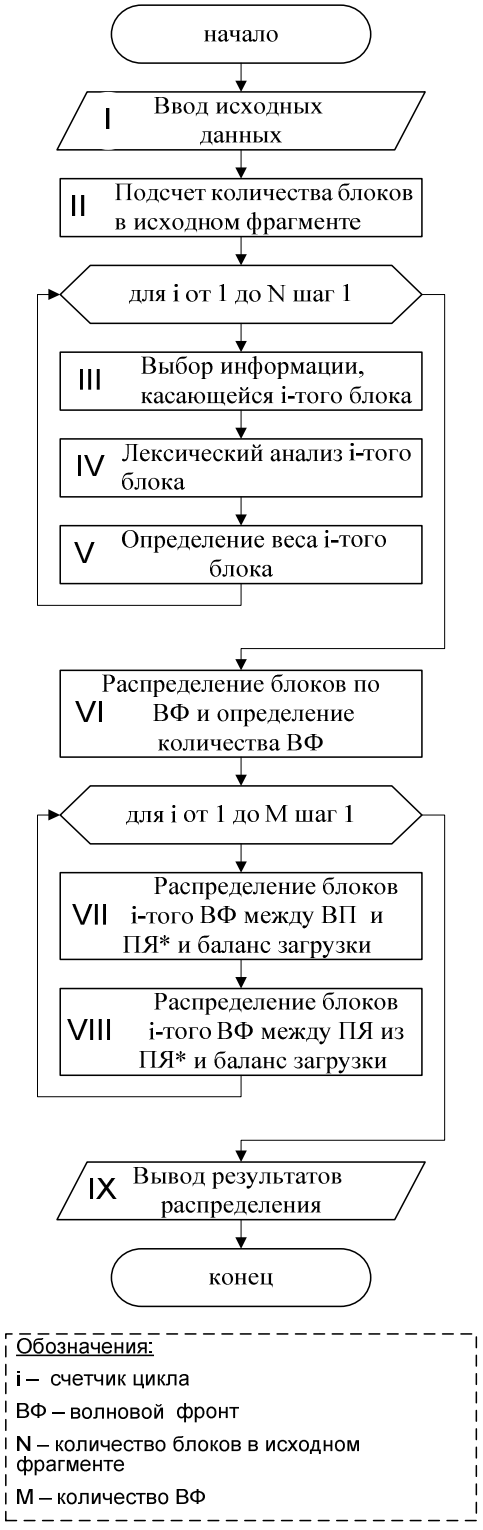


Рисунок 1 – Фрагмент алгоритма распределения приложения

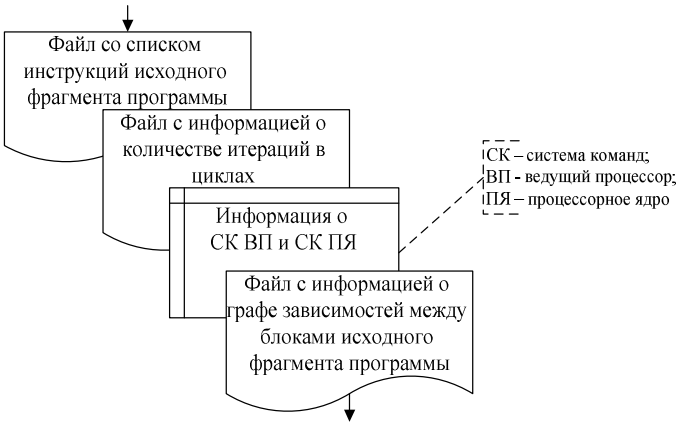


Рисунок 2 – Исходные данные

I. Исходные данные.

Блок-схема исходных данных приведена на рисунке 2. К исходным данным, которые необходимы для работы программы, относятся:

I.1. Список команд, входящих в исходный фрагмент программы. Представлен в текстовом файле в следующем виде: идентификатор блока 1, список команд входящих в блок 1, идентификатор блока 2, список команд блока 2 и т. д. При этом к фрагменту программы предъявляется ряд требований, в частности, фрагмент программы пользователя должен быть написан и откомпилирован на C++ и содержать только те команды, которые входят в систему команд (СК) ВП.

I.2. Файл с информацией о количестве итераций для каждого цикла, входящего в исходный фрагмент программы.

I.3. Описание системы команд ВП и ПЯ, хранится в оперативной памяти ВП в виде структур, состоящих из двух полей: код команды и вес команды для соответствующего процессора. Под весом команды для данного процессора понимается время выполнения этой команды на данном процессоре. Причем, предполагается, что система команд ПЯ является подмножеством системы команд ВП .

I.4. Файл с описанием графа зависимости между блоками фрагмента исходной программы. Структура файла следующая: идентификатор вершины, список дочерних вершин, идентификатор следующей вершины, список дочерних вершин и так далее. Пока не будут перечислены все вершины графа. Под вершинами графа здесь понимаются блоки, на которые разбит фрагмент исходной программы. Множество ребер графа - это зависимости между блоками.

II. Подсчет N -количества блоков, входящих в исходный фрагмент.

В данном блоке анализируют файл, содержащий список инструкций исходного фрагмента программы приложения и подсчитано число **N**-количество блоков, входящих в этот фрагмент.

III. Выбор информаии, касающейся I – ого блока.

Из файла I.1. (см. *исходные данные*) выбирают список инструкций, относящихся к i–тому блоку, а из файла I.2. выбирают информацию о количестве итераций для каждого цикла, входящего в состав i-того блока.

IV. Лексический анализ и получение списка токенов блока.

В процессе лексического анализа считывают исходный текст блока, распознают и выделяют лексемы (при этом убираются лишние пробелы и символы табуляции) и выдают последовательность токенов, которая используется в **V** для проверки сооветсвия команд, входящих в данный блок, системам команд ВП и ПЯ и дальнейшего определения возможности выполнения блока на ВП и ПЯ, а также подсчета веса блока для ВП и ПЯ.

Под лексемой здесь понимают последовательность допустимых символов языка С++, имеющая смысл для компилятора.

Токен представлен в виде структуры, которая содержит:

1) идентификатор класса токена (код токена);
2) лексему, выделенную в исходном тексте (необязательный параметр).

Во входном потоке будет существовать целый ряд лексем, для которых на выходе будет получен один и тот же токен. Этот набор лексем описывается правилом (шаблоном), связанным с токеном. В таблице 1 приведены примеры токенов, используемых при работе алгоритма и их описание.

Таблица 1 – Примеры токенов и их описание

Код токена	Неформальное описание шаблона	Примеры лексем
NUM	Любая целая числовая константа	15, 136, -12345
NUM1	Любая числовая константа с плавающей точкой	3.14, -23.002345671
ID	Идентификатор (произвольная последо-вательность латинских букв и цифр, начинающаяся с буквы)	for, sum1, X
COMM	Коментарий(любой набор символов, находящийся между /* и */, или все символы до конца строки, расположенные после //)	/* вычисление веса*/ // количество записей
LIT	ЛИТЕРАЛ (любые символ между парными кавычками или парными апострофами)	"S=%d" 'g' "house"
LOGIC	Логическая операция (&& или || или !)	&&, ||
REL	Отношение сравнения(== или > или < или >= или <= или !=)	>,>=
OP	Арифметическая операция (+ или - или * или / или % или INC или DEC)	+, DEC
BI	Побитовая операция ()	&, ^
…	…	…
ER	При выдедлении лексемы найдена ошибка	
NONE	Входая лексема не относится ни к одному из вышеперечисленных токенов	

V Определение веса блока. Вес каждого блока вычисляют в виде пары чисел ($W_{ВП}$, $W_{ПЯ}$), где $W_{ВП}$ – время выполнения блока на ВП, а $W_{ПЯ}$ – время выполнения блока на ПЯ, при этом если значение $W_{ПЯ}$ – окажется равным -1, то выполнение данного блока на ПЯ невозможно.

В процессе анализа списка токенов поочередно выделяются команды и записываются в таблицу команд блока. Каждая запись данной таблицы состоит из следующих полей:

– код команды;
– вес команды для ВП;
– вес команды для ПЯ;
– L (число, показывающее, сколько раз данная команда будет выполнена в блоке).

Изначально последние три поля таблицы заполнены 0. Для каждой команды проверяется входит ли данная команда в СК ПЯ. Реализация функции для такой проверки представлена на рисунке 3. Эта функция, возвращает значение веса для ПЯ рассматриваемой команды, при отсутствии данной команды в СК ПЯ функция возвращает значение -1.

```
int look_skpp()  // проверка: входит ли данная команда в СК ПЯ
{
 int i,k=-1;
 for(i=0;i<skppnum;i++)
       if (skpp[i].instr ==tokenval) k=i;
 if (k!=-1) return skpp[k].w;
 else return -1;
}

// tokenval –  код команды, поиск которой осуществляется
// skppnum – количество записей в таблице skpp
// skpp – таблица для хранения системы команд ПЯ
```

Рисунок 3 – Поиск команды в СК ПЯ.

При обнаружении очередной команды в списке токенов проверяется есть ли эта команда в таблице команд. Реализация функции для такой проверки представлена на рисунке 4.

```
int lookup(int opcod)
       /* Возвращает p1 - номер записи в таблице команд для opcod */
       /* Возвращает 0, если такой команды в таблице команд нет */
       /* optable -  таблица команд */
{
 int p1;
 for(p1=lastentry; p1>0; p1--)
 if (optable[p1].cod == opcod)
 return p1;
 return 0;
}
```

Рисунок 4 – Поиск в таблице команд

Далее возможны два варианта действий:

1. Такой команды в таблице команд еще нет. В этом случае, в таблицу добавляется новая строка, в первое поле этой строки вносится код команды. Во второе поле из таблицы, описывающей систему команд ВП, выбирается вес данной команды для ВП. Осуществляется поиск в таблице, описывающей систему команд ПЯ (рис. 3), и в третье поле вносится вес команды для ПЯ или -1 (если команда не входит в систему команд ПЯ) Число L равно 1, если команда находится вне циклов или вычисляется в зависимости от количества итераций циклов, внутри которых находится команда.
2. Такая команда в таблице уже есть. В этом случае находится строка таблицы, которая содержит данную команду, и изменяется только число L (увеличивается на единицу или на другое число, в зависимости от того находится ли эта команда внутри циклов (одного или нескольких) или вне циклов вообще).

На основании таблицы команд блока вычисляется вес данного блока для ВП и ПЯ.

Вес для ПЯ вычисляется формуле:

$$W_{ПЯ} = \sum_{i=1}^{n} p_{ПЯ\,i} \times l_i ,$$

где n - количество записей в таблице команд, $p_{ПЯ\,i}$ - вес i -той команды для ПЯ, l_i - сколько раз i- тая команда может быть выполнена в данном блоке

Вес для ВП вычисляется по аналогичной формуле:

$$W_{ВП} = \sum_{i=1}^{n} p_{ВП\,i} \times l_i$$

где n - количество записей в таблице команд, $p_{ВП\,i}$ - вес i -той команды для ВП, l_i - сколько раз i- тая команда может быть выполнена в данном блоке.

Реализация функции для вычисления веса блока приведена на рисунке 5

```
void weightblock()
{ int i;
  WPP=0;WVP=0;
  for(i=1;i<=lastentry;i++)
    {if (optable[i].vp!=-1)
       WPP=WPP+optable[i].vp * optable[i].count;
        else {WPP=-1; break;}
    }
  for(i=1;i<=lastentry;i++)
    {if  (optable[i].pp!=-1)
       WVP=WVP+optable[i].pp* optable[i].count;
       else {WVP=-1; break;}
    }
}
```

Рисунок 5 – Вычисление веса блока

Значение веса для каждого блока сохраняется в специально предназначенном для этого файле. Структура такого файла следующая: идентификатор блока 1, $W_{ВП}$ для блока 1, $W_{ПЯ}$ для блока 1, идентификатор блока 2, $W_{ВП}$ для блока 2, $W_{ПЯ}$ для блока 2, и т.д.

VI Распределение блоков по волновым фронтам и определение количества фронтов волн. На основании графа зависимостей между блоками исходного фрагмента программы (I.4) для каждого блока осуществляется выбор списка родителей, подсчитывается их количество и определяется порядок выполнения каждого блока по индуктивному принципу:

если у блока нет родителей (предшествующих блоков), то его порядок выполнения 0;

для всех остальных блоков порядок выполнения определяется как максимальный порядок выполнения всех родительских блоков (по отношению к данному) плюс один.

Блоки, которые имеют одинаковый порядок выполнения, могут выполняться параллельно и, соответственно, назначаются на один и тот же волновой фронт. Подсчитывается M - количество таких волновых фронтов. Реализация фрагмента программы, в котором показано нахождение порядка выполнения каждого блока, приведена на рис. 6.

```
                                                  . . .
//поиск блоков без родителей, им назначается нулевой порядок выполнения
int flag; // flag - показывает все ли порядки вычислены(0 -все, а -1 нет)
for(i=0;i<=Nodes-1;i++){
if (GR[i].CPAR==0) GR[i].O=0;
else {GR[i].O=-1;flag=-1;}
                        }
int Omax=0; // максимальный порядок блоков, количество фронтов волн определяется как Omax+1
while (flag==-1)
{
         for (i=0;i<Nodes;i++)
           {
              if (GR[i].O==-1)
                {
                   //k - это счетчик родителей
                   int max=-8;//max - максимальный порядок всех родителей
                   for(int k=1;k<=GR[i].CPAR;k++)
                       {
                         if (i==0)l=0;
                         else l=GR[i-1].PINDEX;
                         r=poisk(TIME_PARENTS[l+k-1]);
                         if (GR[r].O==-1){max=-8;break; }
                         if (max<GR[r].O) {max=GR[r].O;};
                       }
                         if (max>=0) {GR[i].O=max+1; if (Omax<max+1){Omax=max+1;};}
                 }
           }
          flag=0;
          for (i=0;i<Nodes;i++){if (GR[i].O==-1) {flag=-1;break;}}
 }
                                                  . . .
```

Рисунок 6 – Определение порядка выполнения блоков

*VII. Распределение блоков і-того волнового фронта между ВП и эквивалентным ПЯ**. Внутри одного волнового фронта те блоки, которые не могут быть выполнены на ПЯ объединяются в один составной блок, который будет выполнен на ВП, вес этого блока равна сумме весов для ВП блоков, входящих в этот составной блок. Все остальные блоки внутри данного волнового фронта назначаются на эквивалентный ПЯ* и упорядочиваются в порядке убывания $W_{ПЯ}$. Выполняется баланс загрузки ВП и ПЯ*: если вес $W_{ВП}$ составного блока, назначенного на ведущий процессор, меньше, чем вес $W_{ПЯ}$ первого блока (с наибольшим весом для ПЯ) назначенного на ПЯ*, и количество блоков назначенных на ПЯ* превышает число ПЯ на кристалле, то на ВП назначаются дополнительные блоки, подходящие по весу.

*VIII. Распределение блоков і-того волнового фронта между ПЯ из ПЯ** Блоки, назначенные для выполнения на ПЯ*, распределяются между всеми ПЯ на кристалле. Выполняется баланс загрузки ПЯ.

IX. Вывод результатов распределения. По окончании работы алгоритма результаты распределения сохраняются в отдельном файле в виде идентификаторов процессоров и списков идентификаторов блоков, назначенных каждому процессору, и затем передаются в память процессоров PIM-системы для параллельной реализации.

Выводы

Приведенный в статье алгоритм является частью программы распределения приложения между процессорами PIM-системы, в основу которой положены предложенная авторами стратегия распределения приложений, новые критерии и принципы распределения, которые в максимальной степени учитывают особенности архитектурно-структурной организации PIM-систем. Это позволяет исключить на начальном этапе распределения множество итераций и тем самым уменьшить время распределения, за счет того, что распределение приложения по процессорам сначала выполняют целенаправленно согласно новому критерию – соответствие системы команд процессоров набору операций распределяемого приложения. Кроме того, сходимость и корректность (точность) алгоритма распределения улучшаются при таком подходе за счет того, что на каждом уровне распределения осуществляют проверку и при необходимости корректировку баланса загрузки процессоров PIM-системы.

Разработанный алгоритм и приведенные в статье фрагменты программ, написанные на языке C++, подтверждают работоспособность программы, а также правильность теоретических и методических положений применительно к процедуре распределения.

Особенности архитектуры PIM-системы и следовательно применимость предложенных решений можно перенести на кластерные классические системы, процессор которых в каждом узле кластера отличается от остальных процессоров этого узла по своим функциональным возможностям и соответственно системой команд. Однако в классических кластерных системах каждый узел кластера выполнен не на одном кристалле как в PIM – системе, а на множестве кристаллов, что сказывается на достижении предельных значений параметров производительности.

Список литературы

1. Яковлев Ю.С. Однокристальные компьютерные системы высокой производительности. Особенности архитектурно-структурной организации и внутренних процессов: монография / Ю.С. Яковлев. – Винница: ВНТУ, 2009. – 294 с.
2. Slo-Li Chu. Exploiting Application Parallelism for Processor-in-Memory Architecture / Slo-Li Chu, Tsung-Chuan Huang // Proc. of National Computer Symposium, Taiwan, 2003, December 18-19. – 2003. – P. 293–303. – Режим доступа: http://dspace.lib.fcu.edu.tw/bitstream/2377/564/ 1/OT_1022003305.pdf . – Дата доступа: 17.08.11.
3. Елисеева Е.В. О распараллеливании пользовательских задач в распределенных компьютерных системах типа “процессор-в-памяти” / Елисеева Е.В. //Математические системы и машины.– № 4, 2010. – С. 68-81.
4. Яковлев Ю.С. Основные принципы и методика распределения приложений в сложных компьютерных системах типа “процессор-в-памяти”/Яковлев Ю.С., Елисеева Е.В.// Управляющие машины и системы.– 2009.– № 6.– С. 56-63.
5. Яковлев Ю.С. Математическая модель и стратегия распределения приложений для интеллектуальной памяти распределенных компьютерных систем / Яковлев Ю.С., Елисеева Е.В.// Математичні машини і системи. – 2009. – № 4. – С. 3-17.

Сведения об авторах

Яковлев Юрий Сергеевич – докт. техн. наук, зав. отделом, Институт кибернетики имени В.М. Глушкова Национальной академии наук Украины, 03680, ГСП, г. Киев, пр. Академика Глушкова, 40, тел. 044-526-32-07, моб: +38-067-408-59-07, e-mail: jakus@bigmir.net.

Елисеева Елена Владимировна – молодший науковий співробітник, Институт кибернетики имени В. М. Глушкова Национальной академии наук Украины, 03680, ГСП, г. Киев, Пр. Академика Глушкова, 40, тел. 044-526-32-07, e-mail: evo55555@ukr.net.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056

О.Є. АРХИПОВ, С.М. КУЩ, В.О. ШУТОВСЬКИЙ

Національний технічний університет України «Київський політехнічний інститут», Київ

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МІЖНАРОДНІ СТАНДАРТИ ТА УКРАЇНСЬКЕ ЗАКОНОДАВСТВО

Анотація. Розглянуто вимоги, викладені у нормативних документах, та рекомендації міжнародних стандартів до методики оцінювання ризиків інформаційної безпеки. Наведено умови відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC.

Ключові слова: інформаційна безпека, оцінка ризиків, нормативно-правове забезпечення, українське законодавство, міжнародні стандарти.

Аннотация. Рассмотрены требования, изложенные в нормативных документах, и рекомендации международных стандартов относительно методики оценивания рисков информационной безопасности. Представлены условия соответствия методик оценки рисков информационной безопасности отечественным нормативным документам и международным стандартам ISO/IEC.

Ключові слова: информационная безопасность, оценка рисков, нормативно-правовое обеспечение, украинское законодательство, международные стандарты.

Annotation. The information security risk assessment technique requirements of the Ukrainian legislation acts and international standards are reviewed. The conditions of information security risk assessment technique correspondence to the requirements of the Ukrainian legislation acts and international standards ISO/IEC are given.

Keywords: information security, risks assessment, regulatory support, Ukrainian legislation, international standards.

Вступ

Вдосконалення технологій передачі і обробки інформації, щорічне зростання числа кіберзагроз, необхідність забезпечення інформаційної безпеки незалежно від місця її зберігання є причиною особливої уваги до проблеми оцінки ризиків і вдосконалення систем управління ризиками. За результатами дослідження компанії «Ернст енд Янг» в області інформаційної безпеки (ІБ) за 2009 рік [1], наслідки глобальної економічної кризи змусили керівників великих міжнародних компаній переглянути своє відношення до ІБ, зокрема і до процесу управління ризиками ІБ. Так, наприклад, 50% з опитаних керівників планують в майбутньому збільшити фінансування, а 39% збережуть фінансування на попередньому рівні в цьому напрямі.

У відповідності до стандарту ISO 27001 в моделі PDCA (Plan-Do-Check-Act) (так званий цикл Шухарта-Демінга [2]), що описує циклічний процес забезпечення ІБ, етап оцінки ризиків і прийняття рішень займає основне місце. Державний стандарт України [3], певною мірою відповідає основним міжнародним вимогам у галузі ІБ і містить наступний перелік етапів побудови комплексної системи захисту інформації (КСЗІ):

1. Визначення й аналіз загроз.
2. Розроблення системи захисту інформації.
3. Реалізація плану захисту інформації.
4. Контроль функціонування та керування системою захисту інформації.

Відповідно до Державного стандарту України аналіз і оцінка ризиків (п.1- "визначення й аналіз загроз") є першим етапом побудови комплексної системи захисту інформації. Циклічне проведення оцінки ризиків системи дає можливість проводити контроль її функціонування та оптимізувати КСЗІ за встановленими критеріями. Такий механізм оцінки ризиків дозволяє приймати найбільш ефективні рішення, обираючи оптимальні механізми захисту від загроз і розставляючи пріоритети при створенні системи захисту [4]. Адекватна оцінка ризиків для інформаційно-комунікаційної системи (ІКС) є основною умовою побудови економічно обґрунтованої системи захисту інформації (СЗІ) [5].

Актуальність

Актуальність задачі дослідження метрик безпеки (одною з яких є ризик) відмічена у ряді зарубіжних публікацій [6-8]. Дослідження по цій темі ведуться вже декілька десятиліть, але слід відмітити, що одержано відносно мало результатів, які б виявилися корисними для практичного використання, в той час як метрики безпеки є важливим фактором при прийнятті рішень в області інформаційної безпеки [6]. Так, науково-дослідна рада з інформаційної безпеки уряду США включила проблему метрик безпеки на корпоративному рівні до свого останнього списку проблем [7]. Інститутом захисту інформаційної інфраструктури США метрики безпеки визначені як один з чотирьох науково-дослідних пріоритетів на наступні п'ять-десять років [8]. У аналітичному огляді Національного інституту стандартів і технологій (США) "Напрямки досліджень метрик безпеки" [6] наведено перелік умов, які необхідно враховувати при розробці метрик інформаційної безпеки. Цей перелік визначає широкий діапазон проблем від вико-

ристання економічних індикаторів різного типу до особливостей вимірювання показників ІБ систем різної потужності.

На сьогоднішній день запропоновано багато методик оцінки ризиків, які відображені у стандартах [9,10], викладені у звітах науково-дослідних робіт [11,12] та комплексних робіт, виконаних на замовлення комерційних організацій [13,14]. У цих методиках розглянуто питання аналізу і управління інформаційними ризиками, але вони мають ряд недоліків: є недостатньо ефективними, складними, відірваними від практики або навпаки — пристосованими до конкретної організації і конкретної ІКС. Як зазначено у роботах [15,16], на даний час відсутня універсальна методика, яка є однаково придатною для організацій і компаній різних типів.

Мета

Аналіз вимог, викладених у нормативних документах, та рекомендацій міжнародних стандартів до методики оцінювання ризиків інформаційної безпеки, виділення умов відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC.

Постановка задач

4. Провести аналіз нормативних документів українського законодавства у області оцінки ризиків ІБ.
5. Провести аналіз міжнародних стандартів в області оцінки ризиків ІБ.
6. Сформулювати умови відповідності методик оцінки ризиків інформаційної безпеки вітчизняним нормативним документам та міжнародним стандартам ISO/IEC, провести аналіз напрямів розробки методики оцінки ризиків ІБ.

Аналіз нормативних документів українського законодавства у області оцінки ризиків ІБ

Діяльність юридичних і фізичних осіб у сфері інформаційної безпеки в Україні регламентується системою документів: Законами України, Постановами Кабінету Міністрів, Державними стандартами, нормативними документами технічного захисту інформації (НД ТЗІ).

Розгляд питання оцінки ризиків необхідно починати з визначень базових понять. Однак, у перших вітчизняних документах з ТЗІ [3,17,18] терміни «ризик» та «аналіз ризиків» відсутні взагалі, а управління системою захисту інформації (ЗІ) розглядається виключно як адаптація заходів ТЗІ до поточних завдань ЗІ (п.4.4.1 ДСТУ 3396.0), питання економічної доцільності ЗІ зустрічаються в п.3.2 ДСТУ 3396.1 лише в рамках переліку можливих варіантів постановки задачі ЗІ: мінімальні, допустимі або ж необхідні витрати на ТЗІ, оцінка шкоди від реалізації загроз інформації згадується тільки у якості складової частини моделі загроз п.4.5 ДСТУ 3396.0.

Лише з появою у 1999 р. серії документів з захисту інформації в комп’ютерних системах (КС) від несанкціонованого доступу (НСД) тематика оцінки ризиків в галузі ТЗІ стає легітимною [19,20]. Відповідно до нормативного документу [20] ризик визначається як функція ймовірності реалізації певної загрози, виду і величини завданих збитків. Аналіз ризиків у цьому документі визначається як процес визначення загроз безпеці інформації та їх характеристик, слабких сторін комплексної системи захисту інформації (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації автоматизованої системи. Визначення поняття оцінки ризиків у [20] не наводиться, в той час як воно широко використовується у інших НД ТЗІ та літературі, присвяченій проблемам ІБ. На основі розглянутих визначень можна зробити висновок, що формалізованого визначення ризику і моделі взаємозв’язку процесів задачі управління ризиками не запропоновано, що допускає можливість варіювання трактування цього поняття. В загальному випадку обчислення ризику проводиться на основі ймовірності реалізації загрози (або набору загроз) та відповідних збитків організації. Проте, на сьогоднішній день не існує надійного методу визначення ймовірності реалізації ідентифікованих загроз, а також адекватного методу обчислення повного збитку від їхньої реалізації. Складною є задача доведення повноти множини розглянутих загроз і, відповідно, повноти оцінки ризиків [21].

Серед НД ТЗІ безпосередньо оцінки ризиків стосуються [22-25].

Оцінка ризиків в [22] розглядається як одне з завдань, яке необхідно розв’язати при розробці політики безпеки. Відмічено необхідність проведення оцінки гранично припустимих і реальних ризиків у вигляді ймовірності здійснення загроз впродовж заданого проміжку часу, для чого рекомендується вводити дискретні градації. Ймовірності реалізації загроз визначаються на основі експертних оцінок або евристичних даних. Допускається використання як кількісних, так і якісних шкал. У цьому документі аналіз ризиків розглядається як аналіз ймовірностей реалізації загроз. Окремо вимагається проведення оцінки можливих збитків, пов’язаних з реалізацією загроз, аналогічно аналізу ймовірностей реалізації загроз.

У документі [23] введено порівняльну шкалу для оцінки надійності механізмів захисту інформації в комп'ютерних системах від несанкціонованого доступу. КСЗІ представляється у вигляді сукупності функціональних послуг захисту (ФПЗ), кожна з яких є набором функцій, що дозволяють протистояти певній сукупності загроз. Таким чином, не йдеться про оцінку ризиків для системи як таку, а про доведення

реалізації в системі необхідного набору ФПЗ. Оцінка надійності функціонування ФПЗ у [23] не регламентується і віддається у повноваження Експертної комісії, дії якої регламентуються іншими документами.

Відповідно до нормативного документу [24] перелік основних робіт при формуванні технічного завдання включає експертну оцінку очікуваних втрат у разі здійснення загроз, і вибір необхідних функціональних послуг захисту, а також оцінку вартості і ефективності обраних засобів захисту інформації.

У НД ТЗІ [25] на етапі формування технічного завдання на створення КСЗІ на основі вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків і створення переліку суттєвих загроз передбачається необхідність здійснення аналізу ризиків. На етапі формування політики безпеки передбачається уточнення моделей загроз, потенційного порушника та результатів аналізу можливості керування ризиками.

У 2003-2005 роках в якості державних стандартів України було прийнято переклади стандарту ISO/IEC TR 13335, який містить загально прийняту світову термінологію і підходи до оцінки ризиків. Однак ця термінологія не є гармонізованою з серією НД ТЗІ, а підходи ДСТУ не часто застосовуються на практиці.

На основі аналізу українських нормативних документів в області інформаційної безпеки можна зробити декілька висновків. По-перше, аналіз і оцінка ризиків є невід'ємним етапом проектування системи захисту інформації. По-друге, допускається використання як кількісних, так і якісних шкал, об'єктивних та суб'єктивних підходів до отримання оцінки ймовірностей реалізації загроз. По-третє, відсутній НД ТЗІ, який би регламентував процес оцінки ризиків [26], і на поточний момент відсутня гармонізація між основною масою вітчизняних документів (наприклад, НД ТЗІ) та п'ятьма ДСТУ серії ISO. Таким чином, можна зробити висновок про необхідність досліджень по розробці методики оцінки ризиків інформаційної безпеки

Аналіз міжнародних стандартів в області оцінки ризиків ІБ

Сучасні світові стандарти в області інформаційної безпеки передбачають в якості обов'язкового компонента забезпечення режиму ІБ створення системи управління інформаційною безпекою (СУІБ) або її аналогу. Обов'язковою підсистемою останньої є система управління інформаційними ризиками (СУІР), що може включати як кількісні, так і якісні показники і повинна використовувати прозорі метрики [27]. Міжнародною організацією зі стандартизації (International Organization for Standardization, ISO) розроблено близько сотні стандартів, що стосуються інформаційної безпеки і зокрема оцінки ризиків.

Міжнародний стандарт ISO/IEC 27002:2005 [28] визначає ризик як комбінацію ймовірності події і її наслідків. Аналіз ризиків у [28] визначається як систематичне використання інформації для виявлення джерела і оцінки ступеня ризику, а оцінка ризиків — як цілісний процес аналізу ризиків і оцінки їхньої критичності. Наведені визначення в цілому ідентичні вищенаведеним визначенням вітчизняних НД ТЗІ.

Серія стандартів ISO/IEC 2700x включає рекомендації на основі best practices (найкращих практик світового досвіду) у сфері управління інформаційною безпекою, ризиками та засобами контролю як частини загальної системи управління інформаційною безпекою, побудова і функціонування якої здійснюється на основі оцінки ризиків [4]. Розробка СУІБ узгоджена з розробкою систем забезпечення якості та систем захисту навколишнього середовища. У серії стандартів ISO/IEC 2700x опубліковано 8 стандартів і ще 13 готуються до друку. Головні стандарти серії 2700x ISO/IEC 27001:2005 [2], ISO/IEC 27002:2005 [28] та ISO/IEC 27005:2008 [29] базуються на британському стандарті BS-7799. У стандарті [30] до заходів, необхідних для побудови, технічної підтримки та модернізації системи управління інформаційною безпекою, як важливий пункт, включено оцінку ризиків, яка виконується у два основних послідовних етапи: аналіз ризиків та оцінювання ризиків.

У стандартах [2,28] наведено основні етапи оцінки ризиків для СУІБ, а саме:

- визначення методики оцінки ризиків (зазначається, що можна застосовувати різні методики, але головними вимогами до них, є можливість повторення результату оцінки ризиків і порівняння його з результатами оцінок, отриманими за допомогою інших методик);
- ідентифікація ризиків та їхніх складових (активів організації, загроз, вразливостей системи та їхнього впливу на активи);
- аналіз та оцінка ризиків;
- аналіз та оцінка можливості мінімізації ризиків.

Стандарт [29] присвячено управлінню ризиками інформаційної безпеки. У цьому документі розкрито вище перераховані пункти. Стандарт не регламентує вибору конкретної методології оцінки ризиків, і організація може сама вибирати підхід, який би забезпечував необхідні результати і відповідав описаному у стандарті набору критеріїв. Стандарт не віддає перевагу методикам, які використовують кількісні або якісні оцінки ризиків, і в тому числі передбачає можливість використання декількох методик в процесі оцінки ризиків. У ньому визначається структурована та системна послідовність дій від визначення границь системи до розробки плану обробки ризиків. У додатках до стандарту [29] наведено орієнтовні переліки активів, загроз, вразливостей, можливих підходів до оцінки ризиків, а також можливі обме-

ження застосування контрзаходів. Представляє інтерес використання розглянутого в стандарті підходу по формуванню матриць ризиків. Переліки активів, загроз, вразливостей, наведені у стандарті, можуть бути корисними при розробці методики оцінки ризиків ІБ.

У серії стандартів 2700х описано алгоритм управління ризиками, а також довідковий матеріал, необхідний для проведення розрахунків на різних етапах процесу управління ризиками. Згідно вимог стандарту існує можливість вибору однієї з методик, яка відповідає вимогам документованості, раціональності, всебічності та стабільності.

У стандарті ISO/IEC 13335 “Information technology. Security techniques.” визначено набір настанов по управлінню інформаційною безпекою без побудови СУІБ. У стандарті приведені загальні поняття і описані моделі управління безпекою інформаційно-телекомунікаційних систем. Цей стандарт не пропонує конкретних підходів до управління інформаційною безпекою. Частина перша стандарту ISO/IEC 13335-1:2004 [31] відносить управління ризиками до одного з фундаментальних високорівневих принципів інформаційної безпеки. Ризик визначається через ймовірність події і її наслідки. У стандарті запропоновано чотири можливих стратегії аналізу ризиків (базовий підхід, неформальний підхід, детальний аналіз ризику, комбінований підхід). Докладно описано комбінований підхід, який полягає у застосуванні базового підходу для некритичних підсистем і детального аналізу ризиків для критичних підсистем. Комбінований підхід до оцінки ризиків є оптимальним серед запропонованих у стандарті. У додатках до стандарту наведено довідкові матеріали, в тому числі, приведені табличні методики оцінки ризиків, які можуть бути корисними при розробці та тестуванні власної методики оцінки ризиків. Стандарт ISO/IEC 13335 містить огляд загально прийнятих заходів захисту для забезпечення базового рівня захищеності системи, опис різних шляхів досягнення базової захищеності організації, переваги і недоліки різних підходів до побудови системи захисту інформації. Деякі частини стандарту ISO/IEC 13335 на даний момент втратили чинність і частково були замінені на стандарти ISO/IEC 27005:2008. Тим не менш, переклади стандарту ISO/IEC 13335 прийняті у Росії [9,32,33] та Україні в якості національних стандартів.

Стандарт ISO/IEC 18028:2005 “Information technology - Security techniques - IT network security” розширює набір настанов по управлінню інформаційною безпекою, наведених у стандартах ISO/IEC 27002:2005 та ISO/IEC 13335, деталізуючи особливості функціонування і механізми, необхідні для реалізації захисних заходів і елементів управління у більш широкому спектрі мережевого оточення. Цей стандарт є своєрідною з’єднувальною ланкою між загальними положеннями системи управління безпекою інформаційних технологій та способами їхньої технічної реалізації [34]. Аналіз ризиків та вибір на основі положень цього стандарту методики оцінки ризиків ІБ є найбільш ефективним для при оцінці ризиків у окремих конкретних випадках.

У «Загальних критеріях оцінки безпеки інформаційних технологій» (Стандарті ISO/IEC 15408:2002) визначається набір критеріїв безпеки, за якими проводиться сертифікація програмних продуктів, прийнятих у більшості країн світу. Треба відзначити, що процес оцінки є дорогим і довгостроковим, тому він не знайшов широкого застосування за межами ринку урядових і оборонних програмних продуктів. Для розробки методики оцінки ризиків ІБ цей стандарт практично не використовується [34].

На основі аналізу міжнародних стандартів ISO серії 2700х можна зробити висновок, що методика оцінки ризиків повинна відповідати загальноприйнятим вимогам. Основними з них є обґрунтованість методики, повторюваність результатів та їхнє представлення в такій формі, в якій їх можна порівнювати з результатами, отриманими з використанням інших методик. Загальні принципи побудови методики оцінки ризиків стандарту ISO/IEC 13335 (та його російських аналогів) можна покласти в основу розроблюваної методики оцінки ризиків, а стандарт ISO/IEC 18028:2005 зручно використовувати при оцінці ризиків обчислювальної мережі.

Серед зарубіжних стандартів також слід виділити стандарти оцінки ризиків від провідних організацій в області інформаційної безпеки: стандарт BS 7799 від британського інституту BSI, стандарт BSI-100-4 [35] німецької організації BSI, стандарт NIST SP 800-30 [10].

Стандарт від британського інституту BSI BS 7799 лежить в основі серії стандартів ISO/IEC 2700х, які його на цей момент і замінила. Діючою залишається третя частина стандарту BS 7799-3, хоча більша частина його положень увійшла до міжнародного стандарту ISO/IEC 27005:2008 [34].

Відповідно до стандарту німецької організації BSI BSI-100-4 [35] оцінка ризиків проводиться тільки для додаткових ризиків для систем, до яких висуваються підвищені вимоги до забезпечення інформаційної безпеки [34]. Окрім стандарту інститутом BSI розроблено детальний каталог активів, загроз і контрзаходів IT-Grundschutz [36], який представлено у гіпер-текстовому форматі, при чому обсяг каталогу становить понад 4000 сторінок. Цей каталог є найбільш повним з загальнодоступних і його матеріал слід використовувати при розробці методик аналізу ризиків, управління ризиками та аудиті інформаційної безпеки.

Національний інститут стандартів і технологій США (NIST) розробив і опублікував велику кількість стандартів у різних областях для державних, військових та комерційних організацій. Інформаційній безпеці присвячено серію стандартів 800-. В рамках статті найбільший інтерес представляє стандарт

NIST SP 800-30 [10], який регламентує управління ризиками. Оцінка ризиків у цьому документі є першим пріоритетом серед процесів управління ризиками. Ризик визначається як функція ймовірності реалізації заданого джерела загрози через конкретну потенційну вразливість і результуючого впливу цієї шкідливої події на діяльність організації. У стандарті докладно описано методику управління ризиками на основі якісних шкал оцінки ймовірностей загроз та величини збитків (хоча не виключається можливість використання кількісних шкал), а також табличний метод розрахунку ризиків. Наведено приклади розрахунків для ряду випадків. Ефективність контрзаходів запропоновано по результатам проведення аналізу затрати-вигоди. Методика управління ризиками узгоджена з процесом побудови СУІБ, описаним у стандартах серії 2700х.

Серед перерахованих стандартів перспективними для використання при оцінці і управління ризиками є каталог активів, загроз, вразливостей і контрзаходів IT-Grundschutz [36] та методики стандарту SP 800-30 [10].

Не зважаючи, на існування великої кількості стандартів, що регламентують оцінку ризиків, єдиної формалізованої і загальноприйнятої методики або апарату оцінки ризиків не запропоновано. Методика оцінки ризиків створюється для конкретної інформаційної системи. Основними вимогами до методики оцінки ризиків є її обґрунтованість та повторюваність результатів методики, а також представлення результатів у такій формі, в якій їх можна буде порівнювати з результатами, отриманими з використанням інших методик. Цими вимогами слід керуватися при розробці апарату оцінки ризиків інформаційної безпеки.

Аналіз напрямів розробки методики оцінки ризиків ІБ

У роботі, присвяченій визначенню напрямів досліджень метрик безпеки, наведено перелік вимог, які необхідно враховувати при розробці методики оцінки ризиків [6]:

- визначення надійних оціночних функцій безпеки системи;
- зменшення впливу людського фактору та притаманній йому суб'єктивності у вимірах;
- використання системних та ефективних засобів проведення змістовних вимірювань;
- забезпечення прозорості процесів впроваджуваних механізмів безпеки.

В цьому дослідженні також визначені наступні задачі, які необхідно вирішити при розробці методик оцінки ризиків ІБ:

1. Формалізація моделей вимірювань та метрик безпеки.
2. Збір та аналіз статистичної інформації по загрозах та збиткам від них.
3. Використання інтелектуальних технологій.
4. Використання методик, в яких передбачені прямі вимірювання, та інші.

Серед перерахованих задач виділимо використання інтелектуальних технологій для оцінки ризиків ІБ [37-39]. Основною перевагою застосування таких технологій для вимірювання ризику є зменшення суб'єктивного фактору у процесі оцінки ризиків інформаційної безпеки. Дослідження в області інтелектуальних систем [40] особливо бурхливо розвивалися за останні роки. Головною перевагою інтелектуальних систем перед традиційними системами є відсутність програмування у загально прийнятому вигляді. Замість нього проводиться «навчання системи» і забезпечується можливість її пристосування до умов середовища, що змінюються. Основними областями застосування інтелектуальних систем є: інтерпретація даних, діагностика, моніторинг, проектування, прогнозування, планування, навчання, керування, підтримка прийняття рішень, оптимізація. З середини двадцятого століття було запропоновано, реалізовано і успішно застосовано для розв'язання різних задач наступні основні види інтелектуальних систем:

1) експертні системи;
2) штучні нейронні мережі;
3) нечіткі системи;
4) генетичні алгоритми та еволюційне програмування.

Дослідження по застосуванню інтелектуальних технологій в області оцінки ризиків і розробка апарату оцінки ризиків на основі одного або декількох типів інтелектуальних систем були поведені у роботах [37-39].

Висновки:

4. Задача оцінки ризиків інформаційної безпеки на даний момент не має універсального розв'язку і надзвичайно актуальною, як відзначено у зарубіжних і вітчизняних дослідженнях [6-8,27].
5. В Україні оцінку ризиків регламентує ряд нормативних документів технічного захисту інформації [22-25]. На основі аналізу українських нормативних документів в області інформаційної безпеки можна зробити декілька висновків. По-перше, аналіз і оцінка ризиків є невід'ємним етапом проектування системи захисту інформації. По-друге, допускається використання як кількісних, так і якісних шкал, об'єктивних та суб'єктивних методів визначення ймовірностей. По-третє, відсутній НД ТЗІ, який би регламентував процес оцінки

ризиків [26], і на поточний момент відсутня гармонізація між основною масою вітчизняних документів (наприклад, НД ТЗІ) та п’ятьма ДСТУ серії ISO. Обґрунтована методика оцінки ризиків буде задовольняти вимогам вітчизняних нормативних документів.

6. У серії стандартів ISO 2700x [2,28-30] наведено алгоритм процесу управління ризиками, а також довідковий матеріал, який може використовуватися на різних етапах процесу управління ризиками. Методика оцінки ризиків повинна відповідати загальним вимогам, основними з них є обґрунтованість методики, повторюваність результатів та їхнє представлення у такій формі, в якій їх можна порівнювати з результатами, отриманими з використанням інших методик. Загальні принципи побудови методики оцінки ризиків стандарту ISO/IEC 13335 (та його російських аналогів) можна покласти в основу узагальненої методики оцінки ризиків, а стандарт ISO/IEC 18028:2005 можливо використовувати при оцінці ризиків обчислювальної мережі. Серед розглянутих іноземних стандартів перспективними для використання при оцінці ризиків ІБ є каталог активів, загроз, вразливостей і контрзаходів IT-Grundschutz [36] і методики та підходи стандарту SP 800-30 [10].
7. На основі аналізу принципів, які покладено в основу розробки методики оцінки ризиків інформаційної безпеки визначено, що найбільш перспективним є застосування інтелектуальних технологій, зокрема нейронних мереж, нечітких систем та генетичних алгоритмів, а також гібридних інтелектуальних систем.

Список літератури

1. Outpacing change Ernst & Young’s 12th annual global information security survey [Електронний ресурс] // Home - Ernst & Young - Ukraine [сайт] — Режим доступу: http://www.ey.com/Publication/vwLUAssets/12th_annual_global_information_security_survey_brochure/$FILE/12th%20annual%20global%20information%20security%20survey.pdf (29.06.2010). — Назва з екрану.
2. Information technology — Security techniques — Information security management systems — Requirements: ISO/IEC 27001:2005. — [Чинний від 15-10-2005]. — Женева: [б.в.], 2005. — 42 с. — (Міжнародні стандарти ISO/IEC).
3. Захист інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. — [Чинний від 01-01-1997]. — К.: Держстандарт України, 1996. — 6 с. — (Національні стандарти України).
4. Астахов А. Искусство управления информационными рисками / Астахов А. — М.: ДМК Пресс, 2010. - 312 с.
5. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 30 с. — (Нормативні документи системи технічного захисту інформації).
6. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf (10.06.2010). — Назва з екрану.
7. Hard Problem List, INFOSEC Research Council, November 2005 [Електронний ресурс] // Cyber Security Research and Development Center [сайт] — Режим доступу: http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf (10.06.2010). — Назва з екрану.
8. National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective, The Institute for Information Infrastructure Protection, 2009 [Електронний ресурс] // I3P: Institute for Information Infrastructure Protection [сайт] / Martin N. Wybourne , Martha F. Austin , Charles C. Palmer ; The Institute for Information Infrastructure Protection — Режим доступу: http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf (10.06.2010). — Назва з екрану.
9. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3-2007. — [Чинний від 01-09-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2007. — 84 с. — (Національні стандарти Російської Федерації).
10. Gary Stoneburner. Risk Management Guide for Information Technology Systems . Recommendations of the National Institute of Standards and Technology : NIST SP 800-30 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Gary Stoneburner, Alice Goguen, and Alexis Feringa ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (10.06.2010). — Назва з екрану.
11. Корченко А.Г. Построение систем защиты информации на нечетких множествах / Корченко А.Г. – К.:«МК-Пресс», 2006. – 316 с.
12. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики / Балашов П.А., Кислов Р.И., Безгузиков В.П. // Конфидент. – 2003. – 53,№ 4. – С. 56-60; 54,№ 6. – С. 60-66.
13. Control system cyber vulnerabilities and potential mitigation of risk for utilities, Juniper Networks [Електронний ресурс] // Network Security Solutions - Networking Performance Optimization - Juniper Networks [сайт] — Режим доступу: http://www.juniper.net/us/en/local/pdf/whitepapers/2000267-en.pdf (10.06.2010). — Назва з екрану.
14. More Realistic Estimating: Separating Risks and Opportunities from Uncertainty , An Oracle White Paper , March 2009 [Електронний ресурс] // Oracle | Software. Hardware. Complete. [сайт] — Режим доступу: http://www.oracle.com/us/products/applications/042767.pdf (10.06.2010). — Назва з екрану.
15. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с. - (Информационные технологии для инженеров).
16. Петренко С.А. Новые инициативы российских компаний в области защиты конфиденциальной информации / Петренко С.А., Симонов С.В. // Конфидент. – 2003. – 49,№ 1. –С. 56-62.
17. Захист інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. — [Чинний від 01-07-1997]. — К.: Держстандарт України, 1996. — 6 с. — (Національні стандарти України).
18. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97. — [Чинний від 01-01-1998]. — К.: Держстандарт України, 1997. — 10 с. — (Національні стандарти України).
19. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 21 с. — (Нормативні документи системи технічного захисту інформації).
20. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 30 с. — (Нормативні документи системи технічного захисту інформації).
21. Лукацкий А. О заблуждениях в безопасности, ставших классикой [Електронний ресурс] // Bankir.Ru: Технологии, Риск-Менеджмент, Информационная безопасность [сайт] / Лукацкий А.; Bankir.Ru — Режим доступу: http://www.bankir.ru/technology/article/1367694 (10.06.2010). — Назва з екрану.
22. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-00. — [Чинний від 15-12-2000]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000. — 32 с. — (Нормативні документи системи технічного захисту інформації).
23. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 58 с. — (Нормативні документи системи технічного захисту інформації).
24. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі: НД ТЗІ 3.7-001-99. — [Чинний від 01-07-1999]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. — 14 с. — (Нормативні документи системи технічного захисту інформації).
25. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі: НД ТЗІ 3.7-003-05. — [Чинний від 08-11-2005]. — К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. — 25 с. — (Нормативні документи системи технічного захисту інформації).
26. Єрмошин В. Питання розробки методики оцінки ризиків системи управління інформаційною безпекою / Єрмошин В., Капустян М. // Безопасность информации в информационно-телекоммуникационных системах, сборник тезисов докладов XIII Международной научно-практической конференции. – 2010. – С. 67.
27. Петренко С.А. Анализ рисков в области защиты информации, Информационно-методическое

пособие по курсу повышения квалификации “Управление информационными рисками” / Сергей Анатольевич Петренко. — Санкт-Петербург: ООО «Издательский Дом «Афина», 2009. — 153 с.
28. Информационные технологии. Свод правил по управлению защитой информации : ISO/IEC 27002:2005 . — [Чинний від 01-07-2007]. — М.: “Технонорматив”, 2007. — 183 с. — (Міжнародні стандарти ISO/IEC).
29. Information technology — Security techniques — Information security risk management: ISO/IEC 27005:2008. — [Чинний від 15-06-2008]. — Женева: [б.в.], 2008. — 64 с. — (Міжнародні стандарти ISO/IEC).
30. Information technology — Security techniques — Information security management systems — Overview and vocabulary: ISO/IEC 27000:2009. — [Чинний від 01-05-2009]. — Женева: [б.в.], 2009. — 26 с. — (Міжнародні стандарти ISO/IEC).
31. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management: ISO/IEC 13335-1:2004. — [Чинний від 15-11-2004]. — Женева: [б.в.], 2004. — 33 с. — (Міжнародні стандарти ISO/IEC).
32. Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер: ГОСТ Р ИСО/МЭК ТО 13335-4-2007. — [Чинний від 01-09-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2007. — 107 с. — (Національні стандарти Російської Федерації).
33. Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети: ГОСТ Р ИСО/МЭК ТО 13335-5-2006. — [Чинний від 01-06-2007]. — М.: ФГУП «СТАНДАРТИНФОРМ», 2006. — 40 с. — (Національні стандарти Російської Федерації).
34. Other ISMS Standarts [Електронний ресурс] // ISO27k infosec management standards [сайт] — Режим доступу: http://www.iso27001security.com/html/others.html (10.06.2010). — Назва з екрану.
35. Business Continuity Management: BSI-Standart 100-4. — [Чинний від 01-11-2008]. — Бонн: [б.в.], 2008. — 120 с.
36. BSI: IT-Grundschutz-Kataloge [Електронний ресурс] // BSI: Homepage [сайт] — Режим доступу: https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/kataloge.html (10.06.2010). — Назва з екрану.
37. Корченко А.Г. Построение систем защиты информации на нечетких множествах / Корченко А.Г. – К.:«МК-Пресс», 2006. – 316 с.
38. Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики / Балашов П.А., Кислов Р.И., Безгузиков В.П. // Конфидент. – 2003. – 53,№ 4. – С. 56-60; 54,№ 6. – С. 60-66.
39. Кущ С.М. Застосування генетичних алгоритмів для оптимізації нечіткої системи кількісної оцінки ризиків / Кущ С.М., Шутовський В.О. // VII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». Збірка тез доповідей. – 2010. – С. 156-157.
40. Гаврилова Т. А. Базы знаний интеллектуальных систем / Гаврилова Т. А., Хорошевский В. Ф. — СПб.: Питер, 2000. - 384 с.

Відомості про авторів

Архипов Олександр Євгенович – д.т.н., професор, директор Навчального центру перепідготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна.

Кущ Сергій Миколайович – к.т.н., доцент кафедри фізико-технічних засобів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна, тел.:(044) 406-81-04.

Шутовський Василь Олегович – аспірант, асистент кафедри фізико-технічних засобів захисту інформації, Національний технічний університет України «Київський політехнічний інститут», пр. Перемоги, 37, м. Київ, Україна, тел.:(044) 406-81-04, e-mail: v.shutovskyi@gmail.com.

УДК 629.113.004

В.В. БІЛІЧЕНКО

Вінницький національний технічний університет, Вінниця

ВИБІР НАЙБІЛЬШ ЕФЕКТИВНОГО ПРОЕКТУ СТРАТЕГІЙ ОРГАНІЗАЦІЙНО ТЕХНІЧНОГО РОЗВИТКУ ПІДПРИЄМСТВ АВТОМОБІЛЬНОГО ТРАНСПОРТУ

Анотація. Розглянуто вибір проекту реалізації варіанта стратегії розвитку виробничої системи транспорту. Запропоновано для визначення найбільш ефективного проекту використання нечіткої логіки «метод найгіршого випадку», основу якого складають принцип перетинання нечітких критеріїв Белмана – Заде і 9 – бальна шкала лінгвістичних оцінок Сааті.

Ключові слова: проект, варіант стратегії розвитку, нечітка логіка, виробнича система, критерій вибору.

Аннотация. Рассмотрен выбор проекта стратегии развития производственной системы транспорта. Предложено для определения наиболее эффективного проекта использования нечеткой логики «метод наихудшего случая», основу которого составляют принцип пересечения нечетких критериев Белмана – Заде и 9 – бальная шкала лингвистических оценок Саати.

Abstract. The choice of project of development`s strategy of the production transport`s system is considered. Using fuzzy logic - the «method of the worst case» is offered. The basis of it is principle of crossing of unclear Belmana – Zade`s criteria and 9 ball scale of linguistic estimations of Saati.

Вступ

Сучасний етап розвитку економіки України характеризується збільшенням попиту на вантажні та пасажирські автомобільні перевезення. Вирішення цих задач потребує від автомобільного транспорту відповідних змін та перетворень, які дозволили б йому найкращим чином відповідати потребам сьогодення як по своїй технічній базі, так і по структурі та організації транспортного обслуговування як пасажирів, так і господарюючих суб'єктів. В той же час швидке формування ринку транспортних послуг, зміни конкурентного середовища і конкурентних умов, зумовлюють велику ступінь невизначеності роботи автотранспортних фірм і організацій, а також їх залежність від коливань ринкової ситуації, робить неможливим використання традиційних підходів і методів подальшого їх розвитку. В сучасних умовах автотранспортні підприємства, а тим більше невеликі за розміром автотранспортні фірми щоб досягти успіху в конкурентній боротьбі повинні розробляти та реалізовувати стратегії свого розвитку. За таких умов визначення напрямків розвитку та шляхів досягнення стратегічних цілей набуває особливої актуальності. Їх обґрунтування повинно базуватися на використанні сучасних методів, у тому числі стратегічного управління.

Актуальність

Практика стратегічного управління показує, що формування та вибір стратегій - робота дуже трудомістка і клопітка. Кількість стратегій необмежена. Можна сказати, що чим більше сформовано стратегій, тим менша вірогідність того, що керівництво підприємства упустить найбільш сприятливий варіант при виборі оптимальної стратегії розвитку. Правильний вибір стратегії визначає в подальшому ефективність функціонування виробничої системи.

При використанні тієї чи іншої стратегії розвитку необхідно розглядати можливі варіанти (проекти) реалізації цієї стратегії кількість яких може бути різною. Проект реалізації стратегії розвитку відноситься до інвестиційних проектів. В якості показників ефективності інвестиційних проектів найбільшого поширення набули чистий дисконтований дохід (чиста теперішня вартість проекту), індекс дохідності та внутрішня норма прибутковості (внутрішня ставка дохідності) проекту, термін окупності проекту. [1].

Для оцінки ефективності реалізації стратегій та їх варіантів необхідно враховувати усі наведені вище критерії оскільки оцінити її за якимось одним узагальнюючим критерієм не представляється можливим [1]. Тобто при визначенні найбільш ефективної стратегії розвитку виробничої системи необхідно здійснити багатокритеріальний вибір на кінцевій множині альтернатив. В якості альтернатив в нашому випадку розглядаються варіанти (проекти) реалізації стратегій розвитку.

Для вирішення задачі багатокритеріального вибору на кінцевій множині альтернатив найбільше розповсюдження отримали методи векторної і скалярної оптимізації і метод аналізу ієрархій.

Задача багатокритеріальної векторної оптимізації [2] полягає у пошуку вектора цільових змінних, який задовольняє накладеним обмеженням та оптимізує векторну функцію, елементи якої відповідають цільовим функціям. Ці функції утворюють математичне описання критерію задовільності та, зазвичай, взаємно конфліктують. Тобто «отпимізувати» в даному випадку означає знайти такий розв'язок, за якого значення цільових функцій були б прийнятними для постановника задачі.

Для отримання оптимальних розв'язків часто використовують методи скаляризації [3]. Оскільки цільова функція задачі багатокритеріальної оптимізації має векторні значення, її перетворюють на функцію зі скалярним значенням. Таким чином, задача багатокритеріальної оптимізації зводиться до задачі оптимізації з однією скалярною цільовою функцією.

Метод аналізу ієрархій [4]. це математичний інструмент системного підходу до вирішення складних проблем прийняття рішень. Цей метод не надає особі що приймає рішення «правильне» рішення а

дозволяє в ітеративному режимі знайти такий варіант (альтернативу), який найкращим чином узгоджується з його розумінням проблеми і вимогами до її вирішення. Вирішення задачі пошуку рішення методом аналізу ієрархій передбачає використання процедури парних порівнянь. Ця процедура є досить трудомісткою через наявність в ній дробових елементів.

Наведені вище методи є досить трудомісткими потребують для їх застосування значного часу і великої кількості обчислювальних процедур. Тому їх застосування для вирішення задачі багатокритеріального вибору найбільш ефективного варіанту стратегії розвитку є проблематичним.

Мета

Пошук та обгрунтування простого, зрозумілого та ефективного методу багатокритеріального вибору найбільш раціонального проекту реалізації варіанту стратегії розвитку виробничої системи.

Постановка задачі

В загальному вигляді задачу запишемо наступним чином:

Нехай існує деяка кінцева множина альтернативних стратегій розвитку виробничої системи і проектів (варіантів) їх реалізації яку можна записати у вигляді:

$$B = \left\{ b_{11}, b_{12}, ..., b_{21}, ..., b_{ij} \right\}, (i = 1, ..., n,\ j = 1, ..., m). \quad (1)$$

Де *b*–стратегія розвитку; i – номер стратегії; j – номер варіанту стратегії; n – кількість стратегій; *m*– кількість варіантів стратегії.

Необхідно знайти стратегію та її варіант (проект реалізації) який є найбільш ефективним за прийнятими критеріями.

Розв’язання задачі

Множину критеріїв вибору найбільш раціональної стратегії або її варіанту (проекту) можна представити у вигляді:

$$K = \left\{ k_1, k_2, ..., k_l \right\}, (l = 1, 2, ..., h), \quad (2)$$

де K – критерій вибору оптимального проекту розвитку; k_l – складові критерію; l – номер складової критерію; h – кількість критеріїв.

У випадку, коли важливість усіх критеріїв, що утворюють множину, не є однаковою множину критеріїв необхідно записати у вигляді:

$$K = \left\{ \left(k_1\right)^{\mu_1}, \left(k_2\right)^{\mu_2}, ..., \left(k_l\right)^{\mu_l} \right\}, \quad (3)$$

де μ_l – вага критерію k_l.

Необхідно знайти варіант стратегії який за наведеними критеріями є оптимальним.

Широкого розповсюдження для багатокритеріального вибору альтернатив в умовах невизначеності набули методи що базуються на принципах нечіткої логіки. Для багатокритеріального вибору найкращого проекту розвитку в умовах невизначеності скористаємось методом нечіткої логіки «метод найгіршого випадку», запропонованим в роботі [5], основу якого складають принцип перетинання нечітких критеріїв Белмана – Заде і 9 – бальна шкала лінгвістичних оцінок Сааті. Перевага цього методу полягає в тому що при його використанні не застосовуються трудоємкі процедури пов’язані з побудовою і обробкою матриць парних порівнянь.

Кожний критерій k_l є $K = \left\{ k_1, k_2, ..., k_n \right\}$, будемо інтерпретувати як нечітку множину, що задана на універсальній множині альтернатив $K = \left\{ b_{11}, b_{12}, ..., b_{21}, ..., b_{nm} \right\}$ у вигляді:

$$k_l = \left\{ \frac{(\omega_{11}^l)^{\mu_1}}{b_{11}}, \frac{(\omega_{12}^l)^{\mu_2}}{b_{12}}, ..., \frac{(\omega_{nm}^l)^{\mu_l}}{b_{nm}} \right\},\ l = 1, 2, ..., h, \quad (4)$$

де ω_{nm}^l – ступені належності елементів b_{nm} до нечітких множин, що являють собою числа в інтервалі [0, 1], які можуть враховуватись як вага альтернатив відносно критеріїв k_l. При цьому необхідне виконання умови

$$\omega_{11}^l + \omega_{12}^l + ... + \omega_{ij}^l = 1,\ l = 1, 2, ..., h. \quad (5)$$

У відповідності з принципом Бегмана-Заде [5] оптимальний варіант (проект) розвитку визначається наступним чином:

1. Кожний критерій представляється у вигляді нечіткої множини, заданої на універсальній множині проектів.

2. Шляхом перетинання нечітких множин-критеріїв утворюється нечітка множина потенційно хороших рішень.

3. В нечіткій множині потенційних рішень вибирається проект з найбільшою ступеню належності, цей проект і є оптимальним.

Наведене вище можна представити в графічному вигляді (рис. 1).

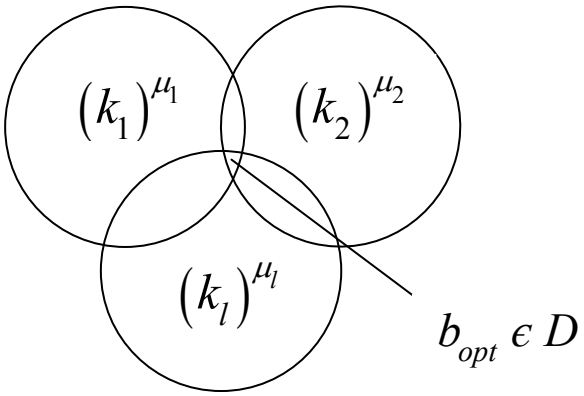


Рисунок 1 – Множина потенційно хороших рішень

Виходячи з цього найкращий проект будемо шукати всередині перетинання ($\cap$) нечіткої множини критеріїв:

$$b_{opt} \in D = (k_1)^{\mu_1} \cap (k_2)^{\mu_2} \cap ... \cap (k_l)^{\mu_l} \tag{6}$$

В теорії нечітких множин має місце заміна операцій: $\cap \to \min$. Виходячи з цього множина потенційно хороших рішень буде мати вигляд:

$$D = \left\{ \frac{\min\left\{(\omega_{11}^1)^{\mu_1}, ..., (\omega_{11}^h)^{\mu_n}\right\}}{b_{11}}, \frac{\min\left\{(\omega_{12}^1)^{\mu_1}, ..., (\omega_{12}^h)^{\mu_n}\right\}}{b_{12}}, ..., \frac{\min\left\{(\omega_{ij}^1)^{\mu_1}, ..., (\omega_{ij}^h)^{\mu_n}\right\}}{b_{ij}} \right\} \tag{7}$$

Як найкращий проект b_{opt} приймається проект $b_{opt} \in D$ з максимальною вагою:

$$\omega(b_{opt}) = \max_{\substack{i=1, 2, ..., n \\ j=1, 2, ..., m}} \min\left\{(\omega_{ij}^1)^{\mu_1}, (\omega_{ij}^2)^{\mu_2}, ..., (\omega_{ij})^{\mu_n}\right\} \tag{8}$$

Визначення ваги всіх проектів (альтернатив), що входять до нечіткої множини (4) базується на ідеях методу структурного аналізу систем [6], в якому належність системи розповсюджується між її елементами відповідно з рангами. Ранг елемента характеризує його важливість в сенсі надійності. В нашому випадку сума ваг, яка дорівнює одиниці буде розподілятись між проектами відповідно до їх рангів.

Нехай q_{ij}^l – ранг проекту $b_{ij}^l \in B$ у відношенні критерію $k_l \in K$. Припустимо наступне: чим вище вага ω_{ij}^l проекту, тим вище його ранг q_{ij}^l. Це формально можна записати у вигляді:

$$\frac{\omega_{11}^l}{q_{11}^l} = \frac{\omega_{12}^l}{q_{12}^l} = ... = \frac{\omega_{ij}^l}{q_{fg}^l} = ... = \frac{\omega_{ij}^l}{q_{ij}^l}. \tag{9}$$

Нехай b_{fg}^l найгірший проект (за критерієм $k_l \in K$) з вагою ω_{fg}^l і рангом q_{fg}^l. Використовуючи співвідношення (9) виразимо ваги усіх проектів через вагу найгіршого проекту:

$$\omega_{11}^l = q_{fg}^l \frac{\omega_{fg}^l}{q_{11}^l}, \quad \omega_{12}^l = q_{fg}^l \frac{\omega_{fg}^l}{q_{12}^l}, ..., \quad \omega_{nm}^l = q_{nm}^l \frac{\omega_{fg}^l}{q_{fg}^l}. \tag{10}$$

Підставляючи ваги проектів в умову $\omega_{11}^l + \omega_{12}^l + ... + \omega_{ij}^l = 1$, отримаємо вагу найгіршої альтернативи за критерієм k_l:

$$\omega_{fg}^l = \frac{1}{\frac{q_{11}^l}{q_{fg}^l} + \frac{q_{12}^l}{q_{fg}^l} + ... + \frac{q_{nm}^l}{q_{fg}^l}} = \frac{1}{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{q_{ij}^l}{q_{fg}^l}}. \quad (11)$$

Співвідношення (10), (11) дозволяють розрахувати вагу проектів через співвідношення рангів кожного проекту q_{ij} до рангу найгіршого проекту q_{fg}. Відмітимо, що порівняння з найгіршим випадком забезпечує виконання умови $\frac{q_{ij}^l}{q_{fg}^l} \geq 1$ для усіх значень $i = 1, ..., n,\ j = 1, ..., m$.

Для визначення співвідношень $\frac{q_{ij}^l}{q_{fg}^l}$ скористаємось дослідом Сааті [7] згідно з яким для кожного критерію $k_l \in K$ задається співвідношення рангів проектів наступним чином:

$$\frac{q_{ij}^l}{q_{fg}^l} = \begin{cases} 1, \textit{ якщо } b_{ij}^l \textit{ співпадає з } b_{fg}^l; \\ 2, \textit{ якщо } b_{ij}^l \textit{ трохи краще за } b_{fg}^l; \\ 5, \textit{ якщо } b_{ij}^l \textit{ краще за } b_{fg}^l; \\ 7, \textit{ якщо } b_{ij}^l \textit{ значно краще за } b_{fg}^l; \\ 9, \textit{ якщо } b_{ij}^l \textit{ абсолютно краще за } b_{fg}^l; \\ 2, 4, 6, 8 - \textit{проміжні значення.} \end{cases}$$

Використовуючи наведені співвідношення, підставляючи отримані значення в формули (10) для усіх критеріїв ми можемо записати критерії як нечіткі множини, задані на універсальній множині проектів (альтернатив). Для визначення найкращого проекту необхідно врахувати вагу кожного з критеріїв.

Для визначення ваги критеріїв μ_k скористаємось принципами і припущеннями наведеними вище. Припускатимемо, що чим вище вага μ_l критерію $k_l \in K$, тим вище його ранг J_l, тобто

$$\frac{\mu_1}{J_1} = \frac{\mu_2}{J_2} = ... = \frac{\mu_q}{J_q} = ... = \frac{\mu_l}{J_l}. \quad (12)$$

Нехай μ_q і J_q - вага і ранг найменш важливого критерію. Тоді вимагаючи виконання умов $\mu_1 + \mu_2 + ... + \mu_l = 1$ по аналогії з наведеним вище при визначенні ω_{ij} розподілимо ваги критеріїв відповідно їх рангам.

$$\mu_q = \frac{1}{\frac{J_1}{J_q} + \frac{J_2}{J_q} + ... + \frac{J_l}{J_q}} = \frac{1}{\sum_{l=1}^{h}\frac{\mu_l}{\mu_q}}. \quad (13)$$

$$\mu_1 = \mu_q \frac{J_1}{J_q}, \quad \mu_2 = \mu_q \frac{J_2}{J_q}, ..., \quad \mu_l = \frac{J_l}{J_q}, \quad (14)$$

де співвідношення рангів критеріїв оцінюється за 9-бальною шкалою:

$$\frac{J_l}{J_q}=\begin{cases}1, \textit{якщо важність критеріїв } k_l \textit{ і } k_q \textit{ співпадають};\\ 3, \textit{якщо } k_l \textit{ трохи важливіше чим } k_q;\\ 5, \textit{якщо } k_l \textit{ важливіше чим } k_q;\\ 7, \textit{якщо } k_l \textit{ значно важливіше чим } k_q;\\ 9, \textit{якщо } k_l \textit{ абсолютно важливіше чим } k_q;\\ 2,4,6,8 - \textit{проміжні значення}.\end{cases}$$

Використовуючи наведені співвідношення за формулами (10), (11) визначаємо вагу μ_l критерію k_l. Виконуючи операцію перетину отриманих нечітких множин отримаємо нечітку множину рішення залежність (8) і визначимо оптимальний проект розвитку виробничої системи у відповідності з залежністю (7).

Розглянемо визначення найбільш ефективного проекту логанізаційно-технічного розвитку Вінницького АТП 10554. В якості можливих прийнято наступні проекти.

Проект b_{11} – оновлення парку бензовозів за рахунок придбання автомобілів-тягачів – DAF FT 85.43 OCF (місткість 28 м^3) в кількості 15 одиниць.

Проект b_{12} – оновлення парку бензовозів за рахунок придбання автомобілів МАЗ-5337А/АБЦ (місткість 12 м^3) в кількості 36 одиниць.

Проект b_{13} – розширення парку автомобілів за рахунок придбання бетонозмішувачів на шасі МАЗ-631268 (вантажопідйомність 13 т) в кількості 15 одиниць.

Проект b_{21} – організація перевезень на маршруті № 61 за умови придбання 7 автобусів пасажиромісткістю 45 пасажирів.

Проект b_{22} – організація перевезень на маршруті № 35 за умови придбання 8 автобусів пасажиромісткістю 120 пасажирів і 13 автобусів пасажиромісткістю 45 пасажирів.

Проект b_{23} – створення станції з визначення технічного стану транспортних засобів з пропускною спроможністю 8800 автомобілів.

Проект b_{31} – реструктуризація підприємства ВАТ АТП 10554 шляхом його об'єднання з приватним підприємством «Автотранском» зі створенням юридичної особи.

Проект b_{41} – внутрішня спеціалізація виробничо-технічної бази за умови створення на підприємстві трьох спеціалізованих постів поточного ремонту.

В якості показників ефективності реалізації проектів приймаємо чистий дисконтова ний дохід (ЧДД), індекс дохідності (ІД), внутрішню норму прибутковості (ВНП), термін окупності ($T_{ок}$) [1]. Числові значення показників в розрізі проектів, що розглядаються, наведені в таблиці 1.

Таблиця 1

Показники ефективності проектів

Показники проекту	ЧДД, грн.	ІД	ВНП	$T_{ок}$, років
Проект b_{11}	6729604	1,51	0,39	2,38
Проект b_{12}	4887496	1,25	0,31	2,87
Проект b_{13}	3472762	1,32	0,33	2,72
Проект b_{21}	7673849	3,60	0,710	1,21
Проект b_{22}	18759074	2,46	0,421	1,77
Проект b_{23}	1063317	2,40	0,426	1,81
Проект b_{31}	656778	1,47	0,230	2,95
Проект b_{41}	255754	1,81	0,68	2,4

За критерієм ЧДД у відповідності з даними таблиці 1 найгіршим є проект b_{41}. Визначимо вагу найгіршого проекту за формулою (11):

$$\omega_{41}^1=\frac{1}{6+5+4+7+9+3+2+1}=\frac{1}{37}=0,0270.$$

Тоді

$$\omega_{11}^1=\frac{6}{37}=0,1622;\ \omega_{12}^1=\frac{5}{37}=0,1351;\ \omega_{13}^1=\frac{4}{37}=0,1008;\ \omega_{21}^1=\frac{7}{37}=0,1892;$$

$$\omega_{22}^1=\frac{9}{37}=0,2432;\ \omega_{23}^1=\frac{3}{37}=0,0811;\ \omega_{31}^1=\frac{2}{37}=0,0541.$$

За критерієм ІД найгіршим є проект b_{12}. В цьому випадку отримаємо:

$$\omega_{12}^2=\frac{1}{4+1+3+9+8+7+4+6}=\frac{1}{42}=0,0238.$$

Тоді

$$\omega_{11}^2=\frac{4}{42}=0,0952;\ \omega_{13}^2=\frac{3}{42}=0,0714;\ \omega_{21}^2=\frac{9}{42}=0,2143;\ \omega_{22}^2=\frac{8}{42}=0,1905;$$

$$\omega_{23}^2=\frac{7}{42}=0,167;\ \omega_{31}^2=\frac{4}{42}=0,0932;\ \omega_{41}^2=\frac{6}{42}=0,1428.$$

За критерієм ВНП найгіршим є проект b_{31}, його вага буде складати:

$$\omega_{31}^3=\frac{1}{5+4+4+9+6+6+1+8}=\frac{1}{43}=0,0232.$$

Тоді

$$\omega_{11}^3=\frac{5}{43}=0,1163;\ \omega_{12}^3=\frac{4}{43}=0,0930;\ \omega_{13}^3=\frac{4}{43}=0,0930;\ \omega_{21}^3=\frac{9}{43}=0,2093;$$

$$\omega_{22}^3=\frac{6}{43}=0,1395;\ \omega_{23}^3=\frac{6}{43}=0,1395;\ \omega_{41}^3=\frac{8}{43}=0,1860.$$

За критерієм $T_{ок}$ найгіршим є проект b_{31}.

$$\omega_{31}^4=\frac{1}{3+2+2+9+8+7+1+3}=\frac{1}{35}=0,0286.$$

Тоді

$$\omega_{11}^4=\frac{3}{35}=0,0857;\ \omega_{12}^4=\frac{2}{35}=0,0571;\ \omega_{13}^4=\frac{2}{35}=0,0571;\ \omega_{21}^4=\frac{9}{35}=0,2571;$$

$$\omega_{22}^4=\frac{8}{35}=0,2286;\ \omega_{23}^4=\frac{7}{35}=0,2000;\ \omega_{41}^4=\frac{3}{35}=0,0857.$$

Для визначення найбільш раціонального проекту необхідно визначити вагу кожного з критеріїв, що розглядаються. Вага критеріїв визначається базуючись на аналогічних постулатах за формулою (14).

Найменш важливою складовою критерію в нашому випадку є ІД, його вага буде дорівнювати:

$$\mu_3=\frac{1}{6+1+3+5}=\frac{1}{15}=0,0667.$$

Вага інших складових критерію буде дорівнювати:

$$\mu_1=\frac{6}{15}=0,4000;\ \mu_2=\frac{3}{15}=0,2000;\ \mu_4=\frac{5}{15}=0,3330.$$

Визначаємо вагу кожного проекту з урахуванням ваги критерію $(\omega_{ij}^l)^{\mu_l}$. Результати розрахунків наведено в таблиці 2. Виконуючи операцію перетину нечітких множин $D=ЧТВ\cap ІД\cap ВНП\cap T_{ок}$ отримаємо нечітку множину рішення:

$$Д=\left\{\begin{matrix}\frac{0,4412}{b_{11}};\frac{0,3854}{b_{12}};\frac{0,4106}{b_{13}};\frac{0,5138}{b_{21}};\\ \frac{0,5680}{b_{22}};\frac{0,3661}{b_{23}};\frac{0,3140}{b_{31}};\frac{0,2358}{b_{41}}\end{matrix}\right\}.$$

Аналізуючи нечітку множину можна зробити висновок, що найкращим проектом організаційно-технічного розвитку буде проект b_{22}.

Таблиця 2

Вага проектів з урахуванням ваги критеріїв

Вага проекту	$(\omega_{ij}^1)^{\mu_1}$	$(\omega_{ij}^2)^{\mu_2}$	$(\omega_{ij}^3)^{\mu_3}$	$(\omega_{ij}^4)^{\mu_4}$
Проект b_{11}	0,4831	0,6247	0,8657	0,4412
Проект b_{12}	0,4490	0,4735	0,8529	0,3854
Проект b_{13}	0,4106	0,1898	0,8529	0,3854
Проект b_{21}	0,5138	0,7348	0,9005	0,6361
Проект b_{22}	0,5680	0,7176	0,8769	0,6117
Проект b_{23}	0,3661	0,6991	0,8769	0,5851
Проект b_{31}	0,3114	0,6221	0,7799	0,3061
Проект b_{41}	0,2358	0,6756	0,8939	0,9667

Висновки

Задача вибору найбільш ефективного варіанту (проекту) розвитку виробничої системи відноситься до задач багатокритеріального вибору на кінцевій множині альтернатив. Для вирішення задачі багатокритеріального вибору найкращого проекту розвитку в умовах невизначеності запропоновано використання методу нечіткої логіки «метод найгіршого випадку», основу якого складають принцип перетинання нечітких критеріїв Белмана – Заде і 9 – бальна шкала лінгвістичних оцінок Сааті. Перевага цього методу полягає в тому що при його використанні не застосовуються трудоємкі процедури пов'язані з побудовою і обробкою матриць парних порівнянь. Наведено основні положення цього методу стосовно вирішення задачі що розглядається.

Список використаної літератури

1. Біліченко В. В. Визначення ефективності проектів технічного розвитку виробництва на автомобільному транспорті [Електронний ресурс] / В. В. Біліченко, Є. В. Смирнов // Наукові праці Вінницького національного технічного університету. – 2009. - №2. Режим доступу до журн.: http://www.nbuv.gov.ua/e-journals/VNTU/2009-2/2009-2.files/uk/09vvboat_ua. pdf

2. Хубка В. Теория технических систем / В. Хубка. — М.: Мир. 1987. — 208 с.

3. Подиновский В. В. Парето-оптимальные решения многокритериальных задач : [монография] / В. В. Подиновский, В. Д. Ногин. - 2-е изд., испр. и доп. Москва : Физматлит , - 255 с.

4. Беллман Р. Принятие решений в расплывчатых условиях / Р. Беллман, Л. А. Заде // Вопросы анализа и процедуры принятия решений. М. : Мир, 1976.-С. 172-215.

5. Ротштейн А. П. Нечеткий многокритериальный выбор альтернатив: метод наихудшего случая / А. П. Ротштейн // Изв. РАН. Теория и системы управления. 2009. №3. – С.51-55.

6. Саати Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М.: Радио и связь 1989. – 316 с.

7. Саати Т. Математические методи конфликтних ситуаций / Т. Саати. – М.: Советское радио, 1977. – 304 с.

8. Нечипоренко В. И. Структурний анализ систем: надежность и ефективность / В.И. Нечипоренко. – М.: Советское радио, 1976. 216 с.

Довідка про авторів

Біліченко Віктор Вікторович – к.т.н., професор, завідувач кафедри автомобілів та транспортного менеджменту вінницького національного технічного університету, хмельницьке шосе, 95, м вінниця, 21021, bilichenko_v@mail.ru.

УДК 355.01

А.В. ДУДАТЬЄВ

Вінницький національний технічний університет, Вінниця

ІНФОРМАЦІЙНА БЕЗПЕКА СОЦІОТЕХНІЧНИХ СИСТЕМ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Анотація. У статті розглянуто умови функціонування соціотехнічних систем. Запропоновано структурні моделі механізмів ведення інформаційної війни, які дозволяють забезпечити необхідний рівень інформаційної безпеки сучасного підприємства.
Ключові слова: Інформаційна безпека, соціотехнічні системи, інформаційна війна.
Аннотация. В статье рассмотрены условия функционирования социотехнических систем. Предложены структурные модели механизмов ведения информационной войны, которые позволяют обеспечить необходимый уровень информационной безопасности современного предприятия.
Ключевые слова: Информационная безопасность, социотехническая система, информационная война.
Annotation. Operating of the sociotechnical systems conditions are considered in the article. The structural models of mechanisms are offered prosecutions of information war, which allow to provide necessary informative strength of modern enterprise security.
Key words: Safety of information, sociotechnical system, information war.

Вступ

Сучасна концепція соціотехнічних систем (СТС) в протилежність теорії технологічного детермінізму, яка стверджує односторонню дію технології на людину, грунтується на ідеї взаємодії людини і техніки, тобто на взаємозалежних впливах. Соціотехнічна система складається з таких підсистем: технічна підсистема включає пристрої, інструменти і технології, що перетворюють вхідні дані у вихідні певним способом, який покращує ефективність функціонування системи; соціальна підсистема включає людей, їх знання, уміння, настрій, ціннісні установки, відношення до виконуваних функцій, управлінську структуру, систему заохочень. Основними показниками СТС є: ефективність, керованість, стійкість, надійність. Беручи до уваги те, що процес життєдіяльності СТС відбувається у певному середовищі – навколишньому, виробничому, технологічному тощо, то необхідно враховувати важливі чинники – такі як взаємодію з іншими системами – організаціями, що можуть виступати як конкуренти. Беручи до уваги другий закон Джилба – “Будь-яка система, яка залежить від надійності людини – ненадійна” та інтерпретуючи його на поняття «безпека» і розуміючи, що більшість сучасних СТС функціонує у конкурентному середовищі, можна зробити висновок, що забезпечення достатнього рівня комплексної безпеки є важливою задачею.

Актуальність

Безпека сучасних соціотехнічних систем складається з декількох складових. Найбільш важливими з них є такі: економічна, екологічна, промислова, інформаційна тощо. На перший погляд незалежні складові комплексної безпеки соціотехнічних систем при більш детальному аналізі представляються вже взаємозалежними. Нескладно представити ланцюжок ймовірних ризиків таких подій: порушення інформаційної безпеки призводить до порушення екологічної, промислової безпеки, наприклад, якщо розглядати такі об’єкти, як хімічно-небезпечні або атомні станції. Другий приклад: порушення інформаційної безпеки може призвести до порушення економічної безпеки, якщо розглядати такий об’єкт як певну фінансову установу. Зрозуміло, що таких прикладів можна навести ще багато.

Підсумовуючи наведені приклади, взаємозалежність ризиків різних типів можна представити у вигляді структури, яка зображена на рис.1.

Ядро даної структури складає інформаційна безпека.Це дозволяє стверджувати, що підвищення рівня інформаційної безпеки зменшує ризики економічної, екологічної, промислової тощо.

Мета

Метою даної роботи є аналіз механізмів проведення інформаційної війни між двома конкуруючими об’єктами та структурна формалізація механізмів впливу – агітації та пропаганди й інформаційного протиборства.

Постановка задач

1. Виконати аналіз умов функціонування сучасної СТС як критичної системи в умовах інформаційної війни.
2. Розробити структурну модель механізмів агітації і пропаганди.
3. Розробити структурну модель механізму інформаційного протиборства.

Розв’язання задачі

Одним з головних показників стану будь-якої складної системи є її надійність, для сучасної соціотехнічної системи таким показником є її безпека. Людина, як активний елемент такої системи, впливає різним чином на розвиток такої системи і як наслідок впливає на стан і розвиток оточуючого середови-

ща: техногенного, виробничого, екологічного, інформаційного тощо. Сучасні соціотехнічні системи функціонують в умовах критичних глобальних змін, основними ознаками яких є такі:

- різного роду аварії і катастрофи;
- збільшення використання енергії різного походження;
- погіршення стану екології навколишнього середовища;
- терористичні акти.

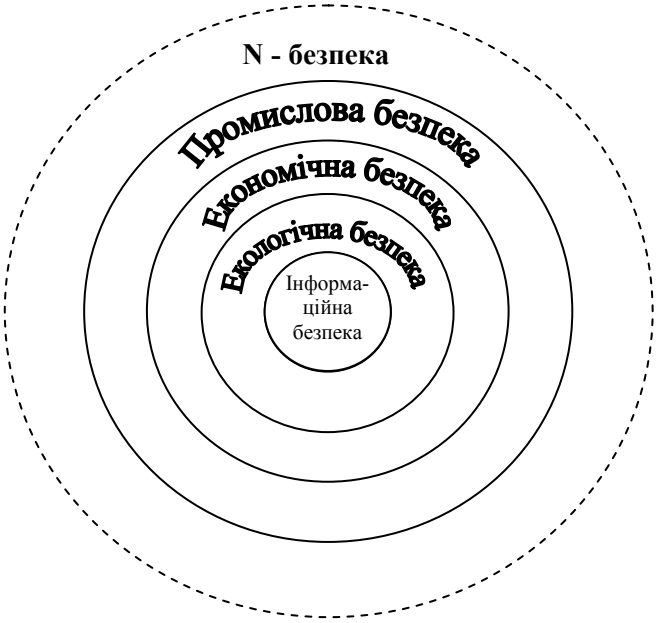


Рисунок 1 – Взаємозалежність ризиків

При цьому життєдіяльність СТС характеризується невизначеністю, яка викликана невчасно отриманою, неповною або навмисно перекрученою інформацією. Варто також відзначити можливість використання конфіденційної інформації потенційними конкурентами у особистих цілях, що вже є ознакою інформаційного протиборства.

В останні часи інформаційне протиборство типу (захист ↔ напад) характеризується елементами інформаційної війни, тобто сукупністю спеціальних операцій, спрямованих на певний об'єкт з метою зміни його стану або структури. Дії, що спрямовуються на об'єкт впливу (ОВ), реалізуються через певну категорію людей або з використанням засобів масової інформації (ЗМІ) завдяки штучній зміні їх свідомості та їх особистого відношення до об'єкту. Суб'єкт, який реалізує спеціальні операції назвемо центром впливу (ЦВ). Таким чином, реалізація технологій інформаційних війн, тобто проведення спеціальних операцій, може бути реалізована за допомогою структури, яка представлена на рис. 2.

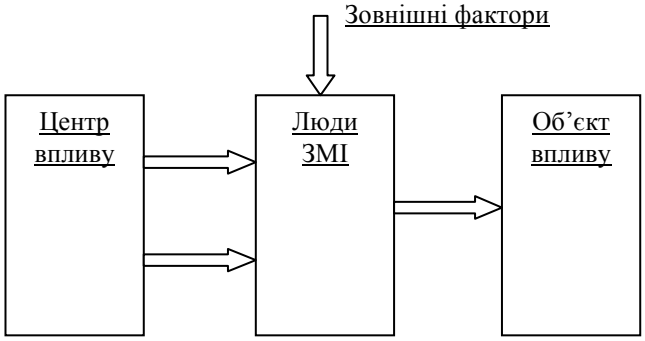


Рисунок 2 – Схема реалізації технологій інформаційної війни

Умовами виникнення інформаційних конфліктів є виборні компанії, боротьба політичних і економічних еліт за сфери впливу, перерозподіл сфер впливу корупційними і кримінальними групами, підготовка і проведення терористичних актів тощо. [1] Загальними передумовами, що можуть спричинити виникнення інформаційної війни, є: розвиток інформаційних технологій, що впливають на свідомість і підсвідомість; практична відсутність інформаційних кордонів; зростаюча роль керівних кадрів, на яких може бути спрямована дія інформаційного впливу. Практична реалізація спеціальних операцій

впроваджується спеціальними структурами – службами безпеки (СБ) об’єктів взаємодії – СБЦВ та СБОВ.

Діяльність служби безпеки спрямована на виконання таких функцій [2]:

- забезпечення захисту власних інформаційних ресурсів;
- забезпечення своєчасного отримання надійної інформації з певних питань;
- забезпечення ефективності та уникнення дублювання при збиранні, аналізі і розповсюдженні інформації.
- моделювання сценаріїв поведінки конкурентів, які можуть стосуватись інтересів підприємства;
- здійснення постійного моніторингу конкурентного середовища;

Ефективність отримання інформації щодо конкурентів досягається шляхом комплексного використання різних засобів і заходів, які забезпечують підвищення достовірності інформації. Технологія отримання інформації передбачає такі етапи:

- організація отримання інформації;
- отримання даних і відомостей;
- проведення інформаційно-аналітичної роботи.

Перераховані етапи отримання інформації мають бути інтегровані в єдиний комплекс і зрозуміло, що всі вони мають велике значення для отримання ефективного результату діяльності СБ об’єкта. Однак, останній етап є найбільш значущим, оскільки результатом проведення інформаційно-аналітичної роботи є звіт, який впливає на прийняття управлінського рішення щодо оцінювання та забезпечення інформаційної безпеки об’єкта. Цей звіт забезпечує керівництво підприємства та його різні підрозділи узагальненою інформацією, яка дозволяю комплексно керувати ризиками різних типів. У практичній площині це дозволяє вирішити такі задачі: проведення інформаційної експрес-оцінки ймовірних конкурентів, та їх можливих дій; інформаційний супровід власних активних дій; комплексний контроль стану захищеності власних об’єктів, ресурсів, комунікацій, конфіденційної інформації; забезпечення координації і взаємодії функціональних підрозділів підприємства на основі взаємного обміну інформацією. Вирішення цих задач дозволяє виявити серед всіх оточуючих об’єктів таких, які мають ознаки зв’язку з ймовірними джерелами загроз – конкурентами, а також ідентифікувати внутрішні загрози, які пов’язані в першу чергу з діяльністю людини. Важливою складовою звіту СБ об’єкта є прогноз поведінки конкурентів і динаміки змін внутрішніх загроз. Це дозволяє з певною достовірністю оцінити можливі сценарії поведінки конкурентів і визначити механізми ведення інформаційної війни. В більшості випадків застосовуються типові схеми дестабілізації об’єкта, які формалізуються у вигляді впливу на людину, дискредитації керівництва об’єкта, інформаційно-психологічного впливу на громадськість відносно об’єкта впливу, а також систематичне розповсюдження спеціально підібраної інформації.

Зрозуміло, що важливою задачею є створення так званого «дружнього інтерфейсу», через який ЦВ зможе реалізовувати свої задачі. При цьому необхідно враховувати, що об’єкт впливу (ОВ) також може знаходитись у двох можливих станах: пасивному і активному. Пасивний стан об’єкта характеризується тим, що він підпадає під повну інформаційну залежність центру впливу, обумовлену тим, що ЦВ має значну перевагу у різних ресурсах: фінансових, інформаційних, ідеологічних тощо. Активний стан об’єкта характеризується тим, що об’єкт проводить відповідні атакуючі або контратакуючі дії.

Розглянемо можливі шляхи реалізації ЦВ своїх задач. Це можуть бути механізми пропаганди, агітації та інформаційного протиборства [3]. Для пасивного стану об’єкта найбільш ефективними є шляхи агітації і пропаганди, оскільки вони спрямовані на зміну свідомості працівників та розповсюдження відповідної інформації, що дозволить змінити стан об’єкту. Інформаційне протиборство передбачає взаємодію конкуруючих структур у боротьбі за лідерство. Зацікавлені люди, як показує практичний досвід, можуть виконувати функції подвійних агентів і реалізовувати як задачі ОВ, так і ЦВ. З урахуванням цього структура інформаційного протиборства представлена на рис.3.

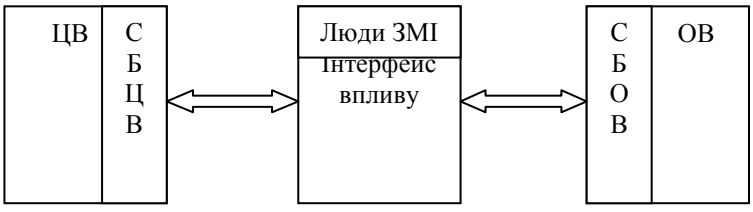


Рисунок 3 – Реалізація інформаційного протиборства

На рис.4 представлена структурна модель реалізації механізмів інформаційного впливу, таких як агітація і пропаганда. Модель враховує створення “дружнього інтерфейсу впливу”, через який підготовлена інформація певним чином впливає на потенційного конкурента. Керівництво об’єкту впливу, вра-

ховує підготовлену інформацію, яка є для нього вхідною і приймає відвідні управлінські рішення, у тому числі щодо забезпечення необхідного рівня інформаційної безпеки.

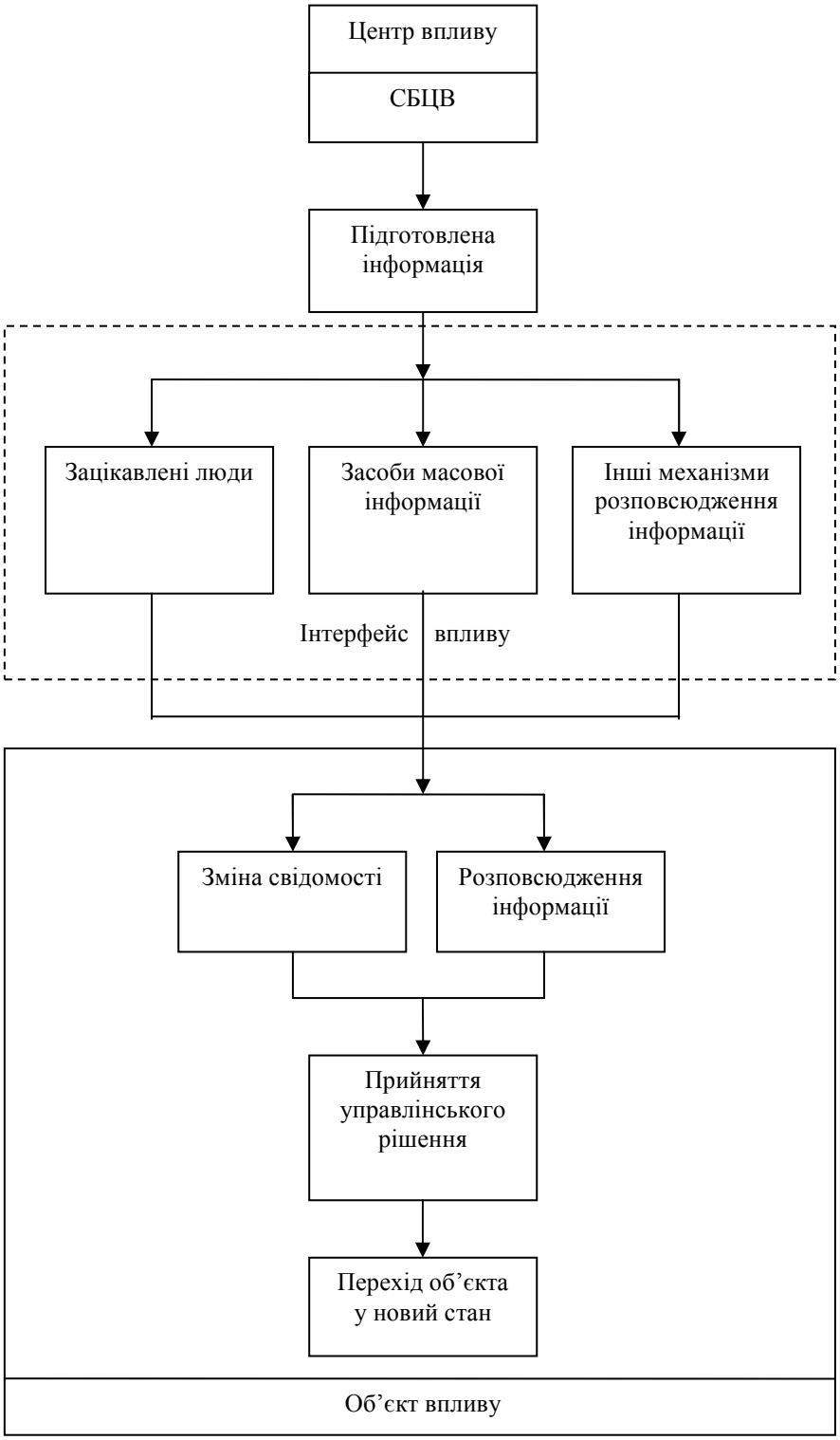


Рисунок 4 – Структурна модель механізмів агітації і пропаганди

Структурна модель реалізації інформаційного протиборства представлена на рис.5 і формалізує процеси взаємодії двох конкуруючих суб'єктів, що можуть призвести до змін інформаційних зв'язків між їх елементами і, як наслідок, зміни їх структури і переходу об'єкта в інший стан. Зміна зв'язків між елементами об'єкта або перехід його у інший стан супроводжується зниженням рівня інформаційної безпеки. Тому для соціотехнічних систем, до яких відносяться і сучасні підприємства, які функціонують

у конкурентному середовищі, важливим є таке правило: “ Необхідно захищати інформацію і захищатись від інформації ”.

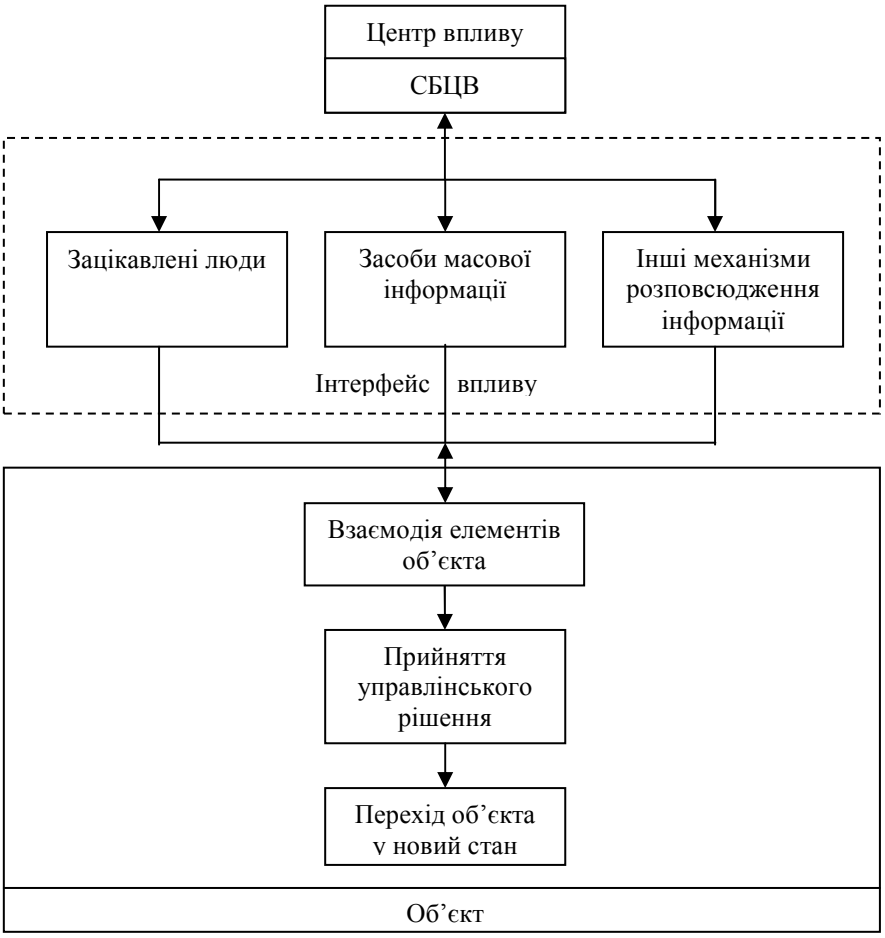


Рисунок 5 – Структурна модель механізму інформаційного протиборства

Висновок

Інформаційні війни є ефективним засобом оволодіння ресурсами. Механізми агітації, пропаганди та інформаційного протиборства забезпечують взаємодію конкуруючих об’єктів із застосуванням елементів інформаційної війни. В статті запропоновані структурні моделі реалізації механізмів ведення інформаційної війни – механізмів агітації і пропаганди та інформаційного протиборства, які можуть використовуватись для досягнення головної мети – забезпечення лідерства на певному сегменті сучасного ринку.

Список літератури

1. Пєвцов Г.В.. Модель регіону України як об’єкту забезпечення інформаційної безпеки / Г.В. Пєвцов // Систми обробки інформації. – Харків.:, 2010. – №5 (86). – С. 2-9.

2. Лужецький В.А. Інформаційна безпека / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця: Універсум-Вінниця, 2009. – 239с.

3. Цыганов В.В. Интелектуальные механизмы информационных войн / В.В. Цыганов, С. Н. Бухарин, В.В. Васин // Проблемы управления. – М.:, 2007. – №1. – С. 25-30.

Відомості про авторів

Дудатьєв Андрій Веніамінович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, вул. Хмельницьке шосе 95, м. Вінниця, Україна (0432) 598485

УДК 004.932.2

Р.Н. КВЄТНИЙ, Ю.В. ПОРЕМСЬКИЙ, М.Ю. ТАРТАЧНИК
Вінницький національний технічний університет, Вінниця

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ РУХУ В ПОТОЦІ ВІДЕО ДАНИХ

Анотація: В більшості країнах світу використовується достатньо велика кількість інформаційних технологій, що застосовуються для обробки, зберігання, ретрансляції та аналізу відео потоків даних. Однією з найскладніших задач щодо обробки відео даних є ідентифікація руху об'єктів в відео потоці. Складність такої задачі полягає у розбитті відео потоку на окремі зображення та аналізу руху об'єктів на кожному окремому зображенні.
Ключові слова: інформаційні технології, відео потік, аналіз руху , ідентифікація руху.
Аннотация: В большинстве стран мира используется достаточно большое количество информационных технологий, применяемых для обработки, хранения, ретрансляции и анализа видео потоков данных. Одной из самих сложных задач по обработке видеоданных является идентификация движения объектов в видео потоке. Сложность такой задачи заключается в разбитии видео потока на отдельные изображения и анализа движения объектов на каждом отдельном изображении.
Ключевые слова: информационные технологии, видео поток, анализ движения, идентификация движения.
Annotation: Most countries used quite a lot of information technologies for processing, storing, analyzing and relaying data video streams. One of the most complex tasks on the video data processing is the identification of moving objects in the video stream. The complexity of this problem lies in the smashing of the video stream into individual images and motion analysis of objects in each image.
Keywords: information technology, video stream, motion analysis, motion identification

Вступ

Проблема ідентифікації руху та виявлення об'єктів в потоці відео даних, на сьогодні, є доволі складною та актуальною задачею в багатьох галузях науки та техніки. Крім того, вона являє собою основу для розв'язання різних типів задач, за рахунок стрімкого розширення області застосування. Як приклади можна навести: охоронні системи, системи відео спостереження в аеропортах та вокзалах, в організаціях боротьби з тероризмом та багато інших. Для розв'язання відповідної задачі більшість інформаційних технологій використовують різні підходи та методики. Класифікації всіх інформаційних технологій та методик, що в них використовуються, надає можливість визначити найбільш функціонально вірну інформаційну технологію.

Отже, метою цієї статті є вирішення актуальної задачі пошуку шляхів підвищення ефективності ідентифікації руху в потоці відеоданих на основі удосконалення існуючих та розробки нових інформаційних технологій.

Актуальність

Вважається, що системи аналізу та ідентифікації руху об'єктів побудовані на звичайному порівнянні певних зображень між собою, але дослідження навіть найпростіших методів та алгоритмів порівняння зображень, показують , що основними складностями в реалізації таких алгоритмів є відсіювання шумів, аналіз статичного фону і т.д. Реалізація найпростіших методів порівнянь зображень дозволяє нам отримати швидкий але менш точний аналіз руху об'єктів, в той час як складні алгоритми (з кращою точністю аналізу), не дозволяють нам використовувати їх в режимі реального часу. Тому, актуальність вдосконалення методів ідентифікації руху об'єктів дуже велика.

Мета

Аналіз запропонованих методів ідентифікації руху об'єктів у відео потоці, класифікації класів рухів об'єктів. Розглянути поширені програмні продукти для ідентифікації руху у відео потоці.

Постановка задачі

1. Проаналізувати методи ідентифікації руху об'єктів у відео потоці.
2. Розглянути класифікацію класів руху об'єктів.
3. Розглянути поширені програмні продукти для ідентифікації руху у відео потоці.

Загальні підходи до розв'язання задачі ідентифікації руху в потоці відео даних

Існують три класи задач обробки та розпізнавання візуальної інформації, що класифікуються як статичні зображення, статичні сцени з елементами руху і тимчасові послідовності зображень. Останній випадок є найскладнішим, оскільки володіє більшою інформативною структурою, а динамічні властивості об'єктів розширюють класичну постановку задач обробки і розпізнавання зображень. Це робить непридатним використання ряду розроблених і добре зарекомендованих класичних методів розпізнавання [1].

Існують різні підходи для ідентифікації руху в потоці відео даних. Всі вони базуються на порівнянні поточного кадру з одним із попередніх кадрів, або з чимось ще, що ми можемо назвати фоном(статичним зображенням).

Методи оцінки руху в потоці відео даних поділяються на методи відповідності та градієнтно-орієнтовні методи для різних груп об'єктів та ситуацій. Методи відповідності [2], представлені на рис. 1, є більш швидкими у виконанні поставленої задачі, але вони менш точні в оцінці руху.

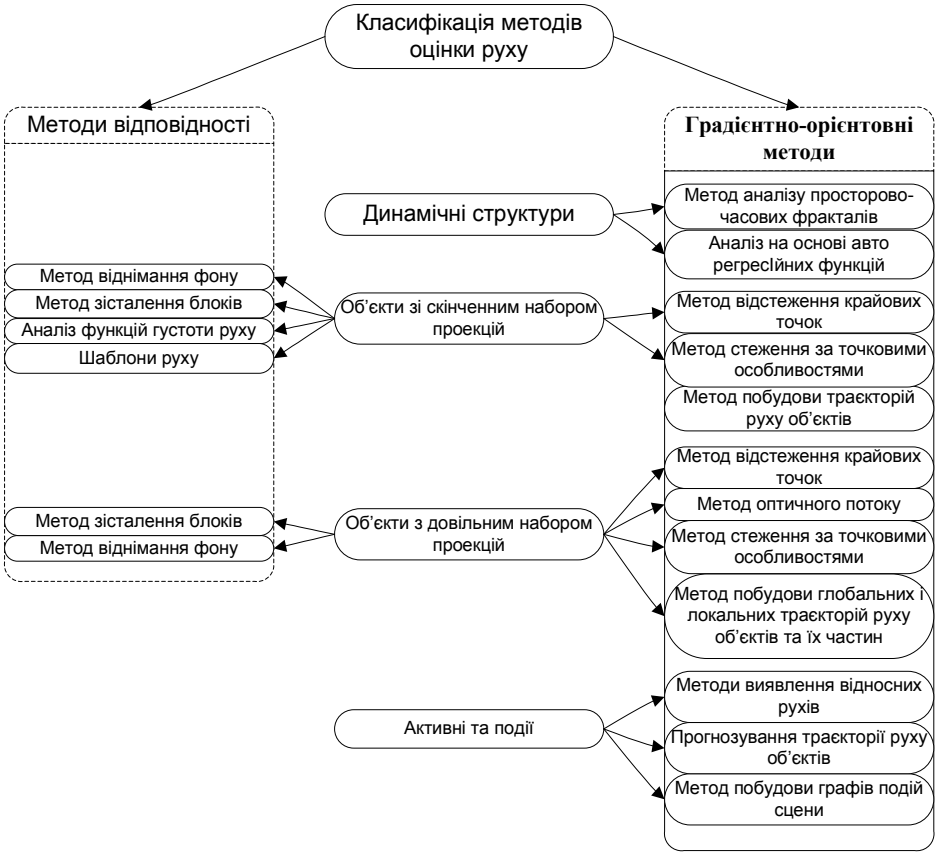


Рисунок 1 – Загальна класифікація методів ідентифікації руху об’єктів в відео потоці даних.

Більшість методів засновано на припущені, що локалізація шаблонів руху приведена до розпізнавання і потрібно встановити відповідність шаблонів для оцінки розташування, швидкості руху і масштабу шаблону на зображенні. Реалізація інших методів потребує визначення точних границь, об’єктів і положення їх частин, як правило, для сцени з простим фоном [3].

Можливість автоматичного формування класів руху об’єктів з тестових вибірок є складною задачею. Рух у відео потоці, з рахунком його повтору в часі та просторі, можна розділити на тимчасові текстури, активні дії, події та складний рух. Класифікація рухів об’єктів в потоці відео даних представлено в таблиці 1.

Таблиця 1 – Класифікація класів рухів об’єктів в потоці відео даних.

Назва	Опис	Область застосування
Тимчасові текстури	Статичні повторення в часі та просторі	Аналіз турбулентності рідин та газів, розпізнавання ландшафтних зображень аналіз руху невеликих однотипних об’єктів
Активні дії	Повторювані в часі структури	Супроводження об’єктів, системи інтерактивної взаємодії людина-комп’ютер (при наявності статичної камери)
Події	Прості рухи які не повторюються в просторі та часі	Аналіз дій людини, пошук в цифрових бібліотеках, аналіз спортивних матчів, відстеження надзвичайних ситуацій
Складні рухи	Динамічні багаторівневі рухи	Аналіз складних сцен при супроводженні об’єктів, навігації роботів, відстеження надзвичайних ситуацій(рухома камера)

Одним з найбільш розповсюджених підходів є порівняння поточного кадру з попереднім. Цей підхід доцільно використовувати тоді, коли необхідно оцінити зміни, та описати тільки зміни, а не весь кадр. Але це не найкращий способом для ідентифікації руху. На цьому етапі ми отримаємо зображення з білими пікселями на місцях, де поточний кадр відрізняється від попереднього на вказані порогові значення. Але, як відомо, більшість камер не надають можливість отримати дійсно якісні зображення(достатньої якості для автоматичної ідентифікації), без великої кількістю шуму, тому ми отримаємо рух в тих місцях де його зовсім не має.

Інші підходи пропонують порівнювати поточний кадр не тільки з попереднім, але й з першим кадром у відео потоці. Таким чином, якщо в початковому кадрі не має об’єктів, то порівнюючи початковий кадр з поточним, ми отримаємо цілий об’єкт, незалежно від швидкості руху самого об’єкту. Але в цьому алгоритмі є певні недоліки. Наприклад, що трапиться якщо, на першому кадрі був автомобіль, а далі його не стало. Тоді на кожному наступному кадрі буде присутній рух, в тому місці де стояв автомобіль. Тому для цього методу нам потрібен статичний фон який не буде змінюватися, наприклад, картина на стелі.

Найбільш ефективні підходи та алгоритми основані на створені так званого фону та порівнянні кожного наступного кадру з фоном. По закінченню процесу заповнення кадру білими та чорними точками починається процес виділення об’єктів. Згусток білих пікселів алгоритм об’єднує в єдиний об’єкт [4].

Інформаційні технології ідентифікації

iSpy — використовує веб-камеру і мікрофон для виявлення, запису рухів та звуків, забезпечує безпеку, спостереження, моніторинг [5]. Також має місце розширена функціональність оповіщення користувача (використовуючи сервіси SMS або ж електронну пошту) – рис. 2 та 3.

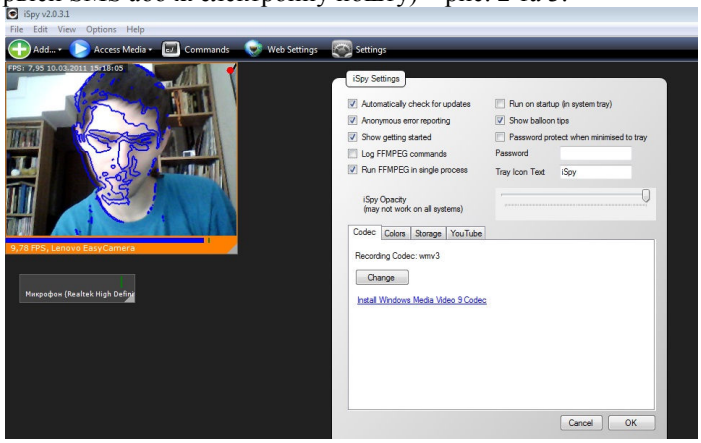


Рисунок 2 – Головне вікно програми iSpy з підключеними камерою та мікрофоном.

Під час виявлення руху, програма починає робити запис, і зберігає його. Будь-який мультимедійний файл, який був збережений інформаційною технологією стискається до флеш-відео або mp4. Крім того він є доступним через глобальну мережу Інтернет, мобільний пристрій або локальну мережу. iSpy може бути налаштований для запуску на декількох комп'ютерах одночасно.

До основних переваг інформаційної технології можна віднести:

1. Додавання необмеженої кількості планів поверху, на яких встановлені камери і мікрофони.
2. Об'єднання відео та аудіо каналів для зйомки відео зі звуком.
3. Запис відео і аудіо за запитом (а також через Інтернет).
4. Підключення декількох комп'ютерів в групу і керування ними через Інтернет.
5. Налаштування виявлення в областях камери.
6. Виявлення і запис звуку.

Основними недоліками ІТ є:

1. Відправлення повідомлень про зафіксовану русі по SMS або електронної пошти платна.
2. При виявленні руху в програмі відображається сам рух що не дозволяє вести приховане спостереження.

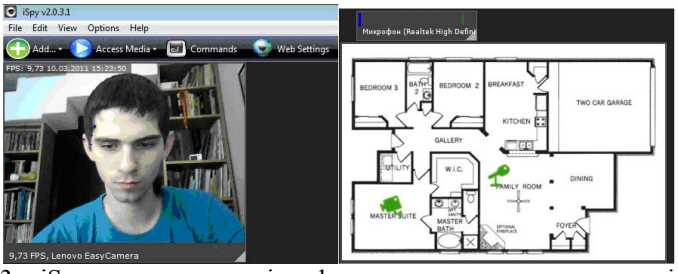


Рисунок 3 – iSpy з камерою та мікрофоном розташованими на плані поверху.

У даному програмному продукті розробники розглянули один з основних методів виявлення руху, це метод порівняння кадру з кадром. Тобто аналітичний центр програми запам'ятовує попередній кадр і порівнює його з поточним кадром. І якщо присутня різниця в цих кадрах, це означає про початок руху об’єкту. За основу такого методу взято використання бінарного зображення як основи руху. Якщо руху

немає і різниця між пікселями поточного і попереднього кадрів дорівнює нулю, то бінарне зображення залишається чорним. В той час, коли з з’являється рух, піксель стає білим і показує об'єкт, що рухається. До найбільш значних функціональних особливостей можна віднести: інформаційна технологія надає можливість розташовувати камери, мікрофони, плани місцевості в довільному та зручному для нас порядку; інтуїтивне меню та панель інструментів;можливий доступ до командної стрічки.

Secure cam

Інформаційна технологія відео спостереження та ідентифікації руху (рис.4). Повідомлення про аварійний сигнал забезпечується електронною поштою, звуковим аварійного сигналу і відеозаписом. Підтримка великої кількості камер. Найважливішими перевагами є:

1. програма проста в налаштуванні функціональності і організації відео спостереження;
2. можливість програми вести приховане спостереження, не показуючи детектора;
3. можливість відправки сигналу про виявлення руху прямо з комп'ютера.

В свою чергу до недоліків можна віднести можливість збереження відео даних при відсутності руху об’єктів [6,7].

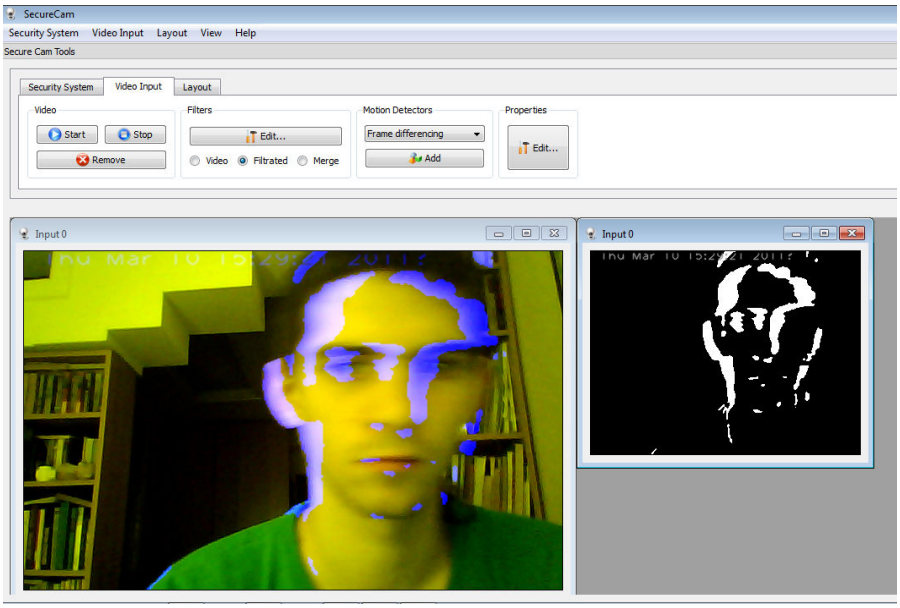


Рисунок 4 – Вікно програми Secure Cam з одною камерою в декількох фільтрах, зліва – камера разом з детектором руху, з права – тільки детектор руху.

Методика детектору руху в Secure Cam так само, як і в попередній інформаційній технології, ґрунтується на порівнянні кадру з кадром. Тому до функціональних особливостей можна віднести: авторизований вхід до програми; наявність видимих фільтрів підключення для обробки зображень; присутність таблиці попереджень про рух; неможливість змінити розмір вікна для відображення камери; можливість використання однієї камери з різними фільтрами обробки зображення.

RiseSun

За допомогою Rise Sun користувач може трансформувати веб-камеру і комп'ютер в систему відео спостереження (рис.5). Rise Sun дозволяє стежити за будинком, офісом або іншим приміщенням. Інформаційна технологія, використовуючи веб-камеру, може зафіксувати будь-який рух об'єктів і автоматично зробити знімок об'єкта, відтворити звуковий сигнал або повністю записати відео [8]. Rise Sun пропонує гнучкі налаштування – надається можливість налаштувати рівень визначення руху, роздільну здатність камери, чутливість сенсорів руху. Інформаційна технологія Rise Sun працює з усіма моделями веб-камер, які доступні на ринку.

Основними перевагами інформаційної технології є:

1. розширені налаштування детекторів руху, щоб враховувати зовнішні, мало значущі чинники, наприклад, рух листя від вітру;
2. автоматичне реагування на рух заданими діями, а саме, автоматичний знімок об'єкта, запис відео, звуковий сигнал;
3. інформаційна технологія має доволі не складний інтерфейс.

В свою чергу найбільшими недоліками є: відсутність відправки оповіщення про рух на електронну пошту; інформаційна технологія працює тільки з однією камерою; камера не повністю захоплює вигляд перед собою, а трохи обрізає його

В даній ІТ представлений більш удосконалень метод ідентифікації руху. Тобто порівнювання поточного кадру з кількома попередніми, що надає можливість виключити з загального аналізу руху переміщення дрібних об'єктів. Функціональні особливостями є: простий інтерфейс; прямий доступ до усіх функцій програми; процентного відображення активності руху відносно зони яку охоплює камера; фіксація часу початку стеження та останнього виявлення руху.

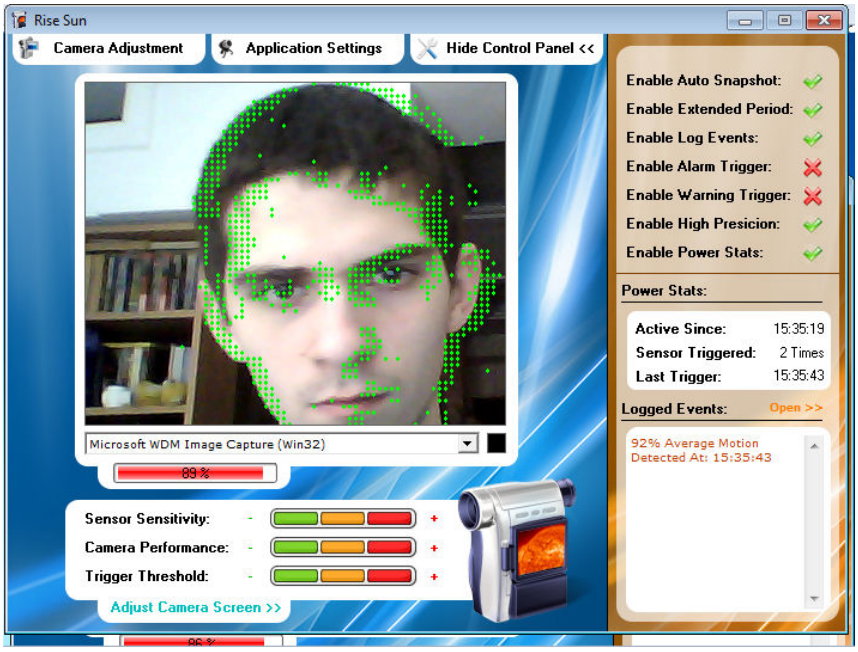


Рисунок 5 – Головний інтерфейс інформаційної технології RiseSun.

OpenCV

OpenCV (англ. Open Source Computer Vision Library, бібліотека комп'ютерного зору з відкритим програмним кодом) - бібліотека алгоритмів комп'ютерного зору, обробки зображень та чисельних алгоритмів загального призначення з відкритим кодом [9]. Поточна версія набору бібліотек, дає можливість розробнику підключати саме ті бібліотеки, які йому потрібні, а не «тягнути за собою» набір не потрібних функцій і методів.

Інформаційна технологія складається з великої кількості модулів, що можуть застосовуватися окремо (таблиця 2).

Таблиця 2 – Основні програмні модулі інформаційної технології OpenCV.

Назва модуля	Опис функціональності
opencv_core	Ядро: базові структури, обчислення(математичні функції, генератори випадкових чисел)) і лінійну алгебру, DFT, DCT, введення / виведення для XML і YAWL і т. д.
opencv_imgproc	обробка зображень (фільтрація, геометричні перетворення, перетворення колірних просторів і т. д.).
opencv_highgui	простий UI, введення / виведення зображень і відео
opencv_ml	статистичні моделі машинного навчання (SVM, дерева рішень, навчання зі стимулюванням і т. д.)
opencv_features2d	розпізнавання і опис плоских примітивів (SURF, FAST і інші, включаючи спеціалізований фреймворк)
opencv_video	аналіз руху і відслідковування об'єктів (оптичний потік, шаблони руху, усунення фону)
opencv_objdetect	виявлення об'єктів на зображенні (перебування осіб за допомогою метода Хара і LBP, розпізнавання людей HOG і т. д.)

продовження таблиці 2

Назва модуля	Опис функціональності
opencv_calib3d	калібрування камери, пошук стерео-відповідності і елементи обробки тривимірних даних
opencv_flann	бібліотека швидкого пошуку найближчих сусідів (FLANN 1.5) і обгортки OpenCV.
opencv_contrib	супутній код, ще не готовий для застосування
opencv_legacy	застарілий код, збережений заради зворотної сумісності.
opencv_gpu	прискорення деяких функцій OpenCV за рахунок CUDA, створений за підтримки NVidia.

В даній збірці модулів для ідентифікації руху використовуються лише наступні: opencv_video(методи оптимізовані саме для виконання своїх функцій); opencv_objdetect (дана бібліотека дозволяє спростити написання програми вже наявними методами, і не треба писати вже написане). Основними функціональними особливостями є :повністю документована бібліотека, що спрощує її використання; наявність прикладів використання функцій та методів; реорганізованість бібліотеки дозволяє підключати потрібні нам модулі без перевищення пам’яті за рахунок не потрібних функцій та методів; бібліотека підтримує багато мов програмування. [10]

Виконаємо аналіз описаних інформаційних технологій щодо основних операції по опрацюванню відео на аудіо потоків даних.

Таблиця 3 – Порівняння основних функціональних можливостей інформаційних технології, щодо обробки відео та аудіо даних.

	ISpy	Secure Cam	RiseSun	OpenCV
Аналіз звуку	+	-	-	-
Захист від руху малих об’єктів	+	-	+	+
Налаштування чутливості	+	+	+	+
Запис відео	+	-	+	+
Попередження про рух	-	+	+	+
Захист від бази даних	+	-	+	+
Підключення великої кількості камер	+	+	-	+
Попередження про рух на незалежний носій	+	+	-	-

Висновок

На даний момент існує достатньо велика кількість інформаційних технології, які вже мають в собі модулі ідентифікації руху, але також є і бібліотеки, які дозволяють удосконалити вже існуючі методи, або створювати нові методи виявлення руху.

Серед наведених ІТ є такі, що краще справляються з ідентифікацією руху у відео потоці, і тому більш підходять для охоронних систем, наприклад ISpy. Але є і такі, що можна використовувати в домашньому використанні, наприклад Secure cam. На даний момент стрімко розвивається тільки OpenCV. Проект вже має значну спільноту розробників, багато опублікованих матеріалів, навіть надруковану O'REILLY книгу, та значну підтримку з боку компанії Intel.

В зв’язку з цим, можна зробити висновок, що кожна з інформаційних технологій, які знаходяться на ринку виконують досить велику кількість задач. Але головним недоліком є відсутність реалізації більшої кількості функціональності в одній інформаційній технології. Також не надається можливість досить швидко модернізувати готові модулі, що підтверджує ізольованість сучасних інформаційних технологій. Тому виникає необхідність в створенні не ізольованих (відкритих до оновлення) інформаційних технологій з ефективним використанням обчислювальних характеристик комп’ютерної техніка, що надасть можливість більш ефективно налаштовувати їх під конкретні задачі.

Список літератури

1. Фаворская М. Н. Модели и методы распознавания динамических образов на основе пространственно-временного анализа последовательностей зображений: автореферат дис. док. тех. наук:

спец. 05.13.17 – «Теоретические основы информатики»/Фаворска Маргарита Николаевна; Сиб. гос. аэрокосмич. ун-т – Красноярск, 2010. – 20 с. : іл., табл. — Бібліогр.: с. 17—18.
2. Фаворская, М.Н. Методы поиска движения в видеопоследовательностях / М.Н. Фаворская, А.И. Пахирка, А.С. Шилов, М.В. Дамов//Вестник Сибирского государственного аэрокосмического университета шимени академіка М.Ф. Решетнева. – Вып. 1 (22) в 2 частях, Ч. 2, Красноярск, 2009. с. 69–74.
3. Фаворская, М.Н. Локальные пространственно-временные признаки событий в видеопоследовательностях // Вматериалах X междунар. науч.-техн. конф. «Теоретические и прикладне вопросы современных информационных технологий», ч. II, Улан-Удэ, 2009. с. 461–466.
4. Фаворская, М.Н. Методы распознавания изображений в видео последовательностей: монография /М. Н. Фаворская; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2010. 176 с.
5. ISpy Connect. — http://www.ispyconnect.com/ — 11.11.2011
6. SecureCam: Project Web Hosting - Open Source Software. — http://securecam.sourceforge.net/ — 11.03.2011
7. Secure Cam Project Solution. — http://sourceforge.net/projects/securecam/ — 15.11.2011
8. Creative software Solution. — http://www.reohix.com/risesun.htm — 11.11.2011
9. OpenCV. — http://opencv.willowgarage.com/wiki/ – 07.11.2011
10. Gary Bradsky. Learning OpenCV / Gary Bradsky, Adrian Kaebler. — O'REILLY., 2008. — 557 p.

Відомості про авторів

Квєтний Роман Наумович – завідувач кафедри автоматики та інформаційно-вимірювальної техніки, доктор технічних наук, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021, тел. 59-85-72.

Поремський Юрій Віталійович – старший викладач кафедри комп'ютерні науки, кандидат технічних наук, Вінницький національний технічний університет, Хмельницьке шосе, 95, м. Вінниця, 21021.

Тартачник Максим Юрійович – студент кафедри аівт, групи 1сі-08, вінницький національний технічний університет, хмельницьке шосе, 95, м. вінниця, 21021, тел. +38-093-037-87-85, e-mail: maxim.tartachnik@gmail.com.

УДК 004.43(031):681.3.01(02)

В.М. ЛУЦЕНКО

Науково-технічний університет України «КПІ», Київ

ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНІЧНИХ ЗАСОБІВ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Анотація. Розглядаэться проблема аналізу властивостей методів та засобів підтримки прийняття рішень для створення проектів систем захисту інформації. Визначено основні властивості таких проектів. Запропоновано підхід до створення нової методики проектування системи захисту інформації від несанкціонованого доступу.

Ключові слова: Захист інформації; комплексна система захисту; асоціативна пам'ять; нейроподібна сіть.

Аннотация. Рассматривается проблема анализа свойств методов и средств поддержки принятия решений для создания проектов систем защиты информации. Определены основные свойства таких проектов. Предложен подход к созданию новой методики проектирования систем защиты информации от несанкционированного доступа.

Ключові слова: Защита информации; комплексная система защиты; ассоциативная память; нейроподобная сеть.

Annotation. The paper considers problem of analyzing of property of means of support of acceptance of decisions for information security systems projects. The basic properties of such projects are given.The technique of complex system designing for non-authorized access protection is developed on the basis of means of support of acceptance of decisions.

Keywords: Protection of the information; complex system of protection; associative memory; neuronal network..

Вступ

Згідно НД ТЗІ 1.1-003-99 [1] несанкціонований доступ до інформації визначається таким чином: НСД до інформації (unauthorized access to information) — доступ до інформації, здійснюваний з порушенням правил розмежування доступу (ПРД). Таке визначення поширюється і на комп’ютерні системи. Причому згідно [2] несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства. Якщо не зосереджуватись на комплексних системах захисту інформації (КСЗІ), а розглядати питання використання систем захисту інформації (СЗІ) у вигляді ще й комплексу технічного захисту інформації на об’єкті інформаційної діяльності згідно положень НД ТЗІ 1.1-005-07 [3], тоді загалом не має значення чи мова йде про захист об’єктів інформаційної діяльності (ОІД) де циркулює інформація з обмеженим доступом (ІзОД), включаючи виділені приміщення (ВП), призначені виключно для проведення конфіденційних переговорів, нарад, доповідей, тощо, чи про автоматизовану систему (АС) як тіло інформаційно-комунікаційної або комп’ютерної системи. Сукупність обох видів об’єктів можна умовно називати об’єктом захисту загальної структури (ОЗЗС). Загальний хід проектування для обох випадків однаковий. Різниця спостерігається у визначенні сенсу та місця рубежу захисту та визначенні сенсу імен і факторів що складають загрози з одного боку та напрямки захисту з визначенням методів і засобів захисту з другого боку. Оскільки створення КСЗІ передбачається як на об’єктах АС і комп’ютерних системах, так і на ОІД (наприклад у ВП), тоді при створенні автоматизованих систем проектування захисту інформації має сенс розглядати КСЗІ (як технічного захисту, так і від несанкціонованого доступу) для ОЗЗС, а не тільки для АС. Згідно з чинниками, визначеними в [4,5], автоматизація проектування системи захисту інформації як технічними каналами так і від НСД на ОІД є завданням проектування складних систем.

Створення складних систем, які передбачають необхідність прийняття рішень при протирічних або неповних даних є напрямком, котрий має тенденцію до розвитку. Це стосується і інформаційно-комунікаційних систем і об’єктів інформаційної діяльності [6,7].

Як зазначено в [5] керований розвиток є процесом, котрий передбачає шлях для досягнення декотрої мети. Наприклад, при створенні методології проектування КСЗІ, ціллю може бути напрацювання комплекту документів, за допомогою яких кваліфікований виконавець здійснює процес проектування. Однак з плином часу умови існування об’єктів інформаційної діяльності такі як зовнішнє середовище, внутрішні властивості, шляхи інформаційних атак, тощо, змінюються. Таким чином, проект захисту та реальні властивості об’єкту, такі як властивості зрілості процесів захисту [8], визначення об’єктивної відповідності моделі загроз умовам існування об’єкту, об’єктивність опису об’єкту що складає його образ [9] при застосуванні методів формалізації опису змінюються безперервно. Крім того, наразі не є реально визначеною кінцева ціль шляху до досконалості проекту КСЗІ, не є навіть визначеною завершеність необхідного переліку безсумнівних властивостей КСЗІ. У таких умовах процес проектування носить дещо випадковий, суб’єктивний характер. Очевидним також є той факт, що реальні проекти за якісними показниками постійно відстають від життєвих вимог.

Іншим підходом на шляху створення єдиної, універсальної та адаптованої до часових змін існування об’єкту системи проектування може бути система, створена на засадах інтелектуальної підтримки прийняття рішень. Така система може використовувати асоціативну пам'ять (АП) з навчанням для визначення шляху трансформації вихідних даних у кінцеве рішення на підставі накопиченого досвіду з проектів реально діючих об’єктів. Звісно, навчанням при цьому є пред’явлення до АП великої (настільки великої, щоб можна було сподіватися на статистичну незалежність окремих проектів) кількості кваліфіковано атестованих діючих проектів. При такому підході принципово можливим є створення єдиної універсаль-

ної та відкритої до розвитку системи. Її якість роботи буде залежати від часу існування, тобто накопиченого досвіду.

Загалом, таке завдання здатне виконуватися з використанням асоціативно-проективних нейроподібних сіток [10]. Головною проблемою при цьому є спосіб формалізованого представлення вихідних, проміжних та кінцевих даних та розробка методу їх кодування.

На перший погляд саме ця проблема і є найбільш нереальною. Мабуть так і є, якщо намагатися створити методологію реалізації проектів виключно на сітках, тобто весь шлях проектування на усіх його етапах здійснювати за рахунок використання єдиної сітьової моделі. Якщо ж розділити проектування на етапи таким чином, що визначеними будуть такі, що піддаються жорсткому алгоритмуванню і такі, що вимагають прийняття квазіоптимальних рішень при протирічних або неповних даних, тоді сіті можна використовувати фрагментарно, без збитків щодо якості проектів.

Одним з проблемних моментів при створенні КСЗІ є створення дієвої структури системи захисту інформації від НСД. Саме цьому моменту присвячена представлена стаття.

Актуальність

Реальні проекти захисту від НСД за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але наразі, як зазначено вище, мають тенденцію до відставання від життєвих вимог. Для подолання такого відставання мають відтворюватися вимоги щодо життєдіяльності системи проектування окремо для кожного об'єкту у повному обсязі. Такі вимоги передбачають необхідність використання системи захисту що базується на принципово об'єктивному проектуванні, тобто такому, котре не залежить від якісних показників проектанта. Спроектована система захисту має бути динамічною у часі, тобто відкритою щодо можливості змін у часі складових методів та засобів захисту або умов існування об'єкту. Також актуальним є питання визначення необхідної та достатньої завершеності проекту системи захисту, а критерії завершеності наразі відсутні. Найголовнішою умовою завершеності проектів є формальна дієздатність системи захисту на даний час та відповідність реалізації спроектованої системи захисту фінансовим можливостям користувача.

Початком більш об'єктивного проектування має бути напрацювання методів та засобів отримання максимально повної та об'єктивної інформації про об'єкт на етапі його дослідження, а також інженерний аналіз для виявлення місць уразливості об'єкту, тобто визначення ступеня його стійкості до загроз.

Мета

Створення дієвої структури системи захисту інформації від НСД за рахунок досконалої системи проектування, принципово об'єктивного та незалежного від вподобань та кваліфікаційних властивостей проектантів.

Постановка задач

Створення життєздатної методики проектування систем захисту об'єктів від НСД, котра відповідає вимогам підвищеної об'єктивності проектів щодо реальних вимог захищеності. При цьому вимоги щодо життєдіяльності системи проектування можуть бути визначеними таким чином:

1. Система має створюватись на базі принципово об'єктивного проектування, незалежного від вподобань та кваліфікаційних властивостей авторів проектів.
2. Система захисту має бути динамічною у часі та відкритою до можливості змін складових бібліотек

методів і засобів захисту або умов життєдіяльності об'єкта, а тому має постійно враховувати його історію.

3. Проект системи має вважатися завершеним при умові, якщо у визначений термін часу повторне незалежне проектування дає однаковий результат. При цьому під визначеним терміном часу слід вважати настільки малий термін, при закінченні котрого властивості об'єкта не змінюються.

Розв'язання задач

Загальний опис структури проектів захисту від НСД є складним і загалом неоднозначним завданням, а створення системи захисту можна звести до етапів:

1. Обстеження інформаційної системи, АС або ОІД з підготовкою базових даних.
2. Розробка технічного завдання на створення системи контролю та обмеження доступу.
3. Розробка проекту.
4. Введення системи захисту в дію та оцінка захищеності.
5. Попередні випробування.
6. Дослідна експлуатація.
7. Експертиза системи відділом служби охорони.

Склад системи також складний. До нього відносять:

1. Службу охорони.
2. Комплекс засобів захисту від несанкціонованого доступу, контролю та обмеження доступу.

3. Інженерно-технічні заходи.
4. Фізичну охорону об’єкту.

При такому визначенні структура процесу моделювання об’єкту захисту має вигляд, як на рис.1.

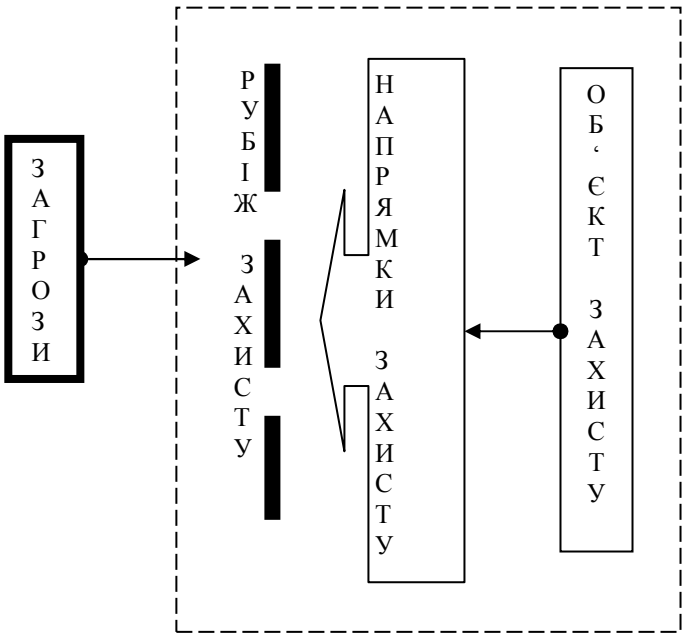


Рисунок 1 – Концептуальна модель процесу захисту інформації від НСД.

Якщо поставити завдання розподілити процес проектування системи захисту за етапами, то загалом зазначені етапи є послідовними багатокроковими процесами з складною структурою. Кожний етап забезпечується великою кількістю методологічних документів, котрі визначають лише загальну методику створення проекту захисту і можливість конкретизації кожного кроку не є реально можливою з причини великого різноманітності параметрів та об’єктів. Наприклад, моделювання методів і засобів захисту від НСД вміщує визначення напрямків захисту, котрі у свою чергу визначають методи захисту, котрі у свою чергу визначають можливі засоби захисту. Останні розділяються на організаційні та технічні. Структура системи захисту від НСД для ОЗЗС має вигляд, як на рис.2.

Очевидно, що автоматизація процесу проектування навіть для такого, найбільш консервативного фрагменту зустрічає складності, наприклад, на етапі визначення пріоритету між випадковими або зловмисними діями порушника, чи розподілі пріоритетів при виборі засобів виявлення факту порушення між фізичною охороною та сигналізацією і відеоспостереженням.

Якщо перенести наведену ілюстрацію на всі етапи напрямків моделювання автоматизованої системи проектування, визначається низка переходів між етапами, де спостерігається невизначеність вибору подальших рішень. На практиці такі завдання щодо прийняття рішень вирішуються за рахунок кваліфікації та вподобань проектанта і згідно його досвіду. В результаті практичні проекти відрізняються невиправданою різноманітністю навіть у майже однакових умовах, а оптимізація проектів як за структурою і використанням засобів захисту, так і за кошторисом залежить виключно від його кваліфікації. З наведеного витікає необхідність створення системи проектування незалежної від користувача та об’єктивно здатної до невипадкової оптимізації рішень але не за рахунок декотрого розробленого алгоритму оптимізації, а за рахунок попереднього досвіду якнайбільшої кількості діючих проектів, тобто статистики вже отриманих рішень.

Так напрямок моделювання загроз складається з двох основних етапів, на основі котрих формується проект захисту, а саме: визначення джерел загроз; визначення моделі порушника, котрий реалізує загрози.

Визначення джерел загроз є фрагментом, котрий піддається жорсткій алгоритмізації і не вимагає втручання моделювання з використанням засобів інтелектуальної підтримки за рахунок сітьового моделювання. Подальший шлях проектування передбачає перехід до моделі порушника з визначенням цілей, на котрі направлені загрози.

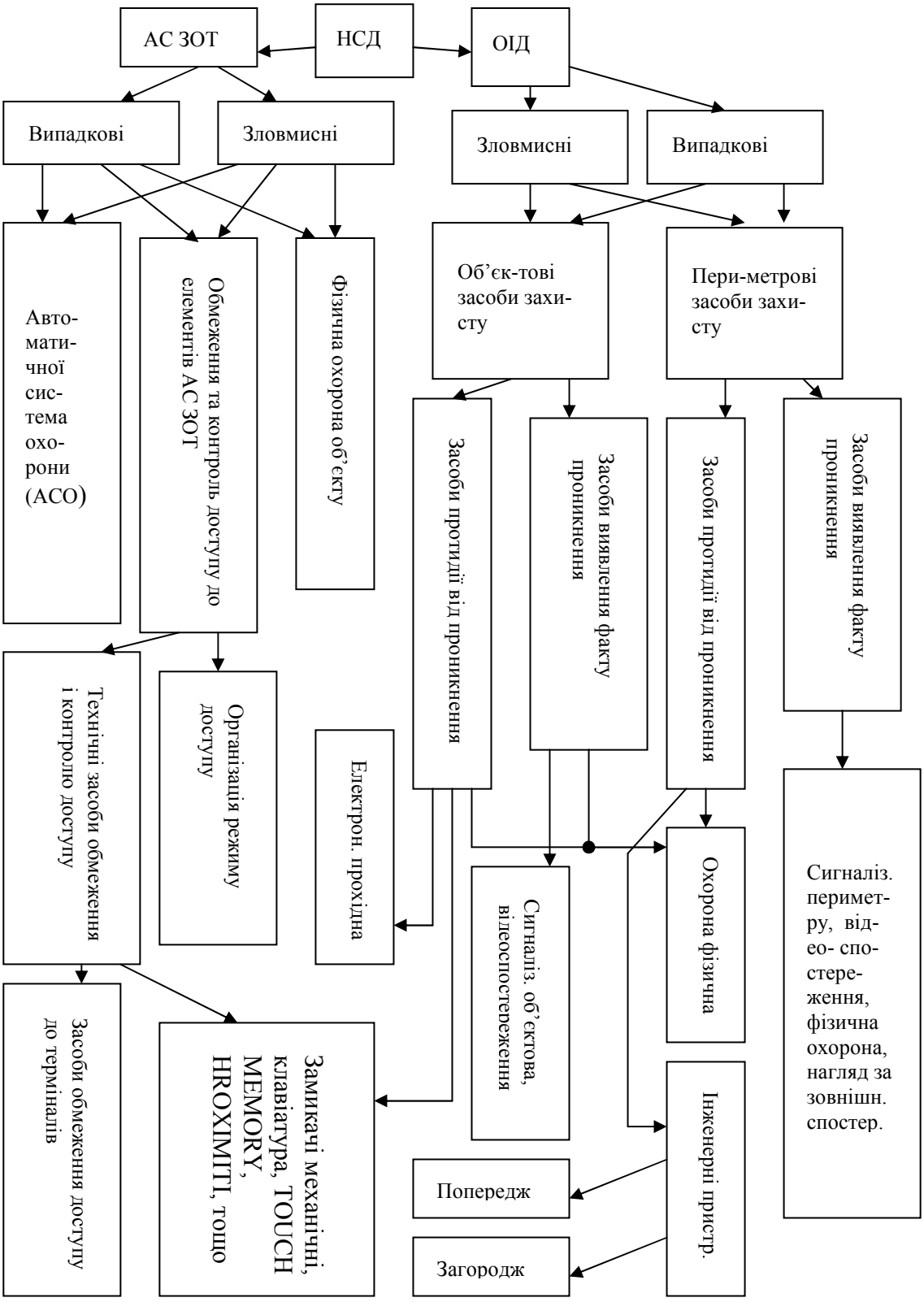


Рисунок 2 – Структура системи захисту ОЗЗС від НСД.

Проведення об'єктивного аналізу цілей загроз для об'єктів середньої та великої складності є завданням нечітким і на цьому етапі використання засобів підтримки прийняття рішень є виправданим. При цьому сукупність цілей загроз об'єкту представляється підмножиною цілей характерних для об'єкту що розглядається, з загальної множини можливих цілей, тобто декотрих елементів образу об'єкту. Особливо вдалим у цьому випадку є те, що при переході від джерел загроз до моделі процедура визначення

цілей загроз є необхідною тільки на попередньому етапі підготовки засобу підтримки прийняття рішень. Наприклад, при використанні в якості засобу підтримки прийняття рішень асоціативної пам’яті на базі моделі нейроподібної асоціативно-проективної ансамблевої сіті [11,12], тоді попереднім етапом підготовки є етап навчання сіті. Тобто проектант захисту об’єкту є звільненим від складання переліку цілей. Його завданням на цьому етапі є тільки опис самого об’єкту без громіздкої та загалом неоднозначної експертизи ступеня його захищеності.

Висновки:

Аналогічно виглядає моделювання наступного етапу, а саме перехід від моделі загроз до напрямків захисту, котрі є головною складовою створення моделі методів і засобів захисту. При цьому в ансамблевому представленні мають бути визначені лише напрямки захисту, що є умовою для реального створення системи проектування.

Декотрі інші етапи проектування системи захисту також можуть моделюватися з використанням засобів підтримки прийняття рішень, що і є предметом поточних розробок фахівців з інформаційної безпеки.

Список літератури

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
3. НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»
4. В.М.Луценко. Система інтелектуальної підтримки прийняття рішень при проектуванні комплексних систем захисту інформації. «Наукові вісті», Наук. Тех.. журнал, НТУУ «КПІ» ВПІ ВПК «Політехніка», 2010, №5, с.с.68-74.
5. Мачуський Є.А., Луценко В.М. Використання елементів засобів інтелектуальної підтримки прийняття рішень при проектуванні систем інформаційної безпеки. X международная научная конференция имени Т.А.Таран «Интеллектуальный анализ информации ИАИ-2010», 18-21 мая 2010 г., Сборник трудов. – К.: «Просвіта», -с.207-213.]
6. ДСТУ ISO/IEC TR 13335:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1: Концепції та моделі безпеки інформаційних технологій. Частина 2: Керування та планування безпеки інформаційних технологій. Частина 3: Методи керування безпекою інформаційних технологій.
7. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
8. Потій О.В. Онтологічні моделі властивостей зрілості процесів захисту інформації. Харьков. Прикладная радиоэлектроника. ISSN 1727-1290. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. 2009г., т. 8, №3, с.388-395.
9. Ayaz Isazadeh. Behavioral Views for Software Requirements Engineering. A thesis submitted to the Department of Computing and Information Science in conformity with the requirements for the degree of Doctor of Philosophy Queen's University Kingston, Ontario, Canada, September 1996. (Досяжні в Інтернет www.sciencedirect.com).
10. Байдык Т.Н. О возможной организации системы принятия решений – В кн. Нейроподобные сети в робототехнике. – Киев: ИК АН УССР, 1979, с. 58-72.
11. J.J. Hopfield, D.W. Tank. “Neural” Computation of Decisions in Optimization Problems. “Biological Cybernetics”, vol. 52, No 3, 1985, p. 136,141-152.
12. Амосов Н.М., Касаткин А.М., Касаткина Л.М., Куссуль Э.М. Нейроподобные сети в системах искусственного интеллекта. Нейроподобные сети и нейрокомпютеры: Сб науч тр. / АН УССР. Ин-т кибернетики им. В.М. Глушкова. Науч. Совет АН УССР по пробл. «Кибернетика». – Киев, 1990. – с. 4-13.

.

Відомості про авторів

Луценко Володимир Миколайович – доцент фізико-технічного інституту (ФТІ) , докторант ФТІ НТУУ «КПІ», в.о. завідувача каф. Фізико-Технічних Засобів Захисту Інформації, кандидат технічних наук, Київ-03056, Проспект Перемоги 37, корп.11. тел. (044) 406-81-04, 097-7962914. e-mail: tarcomevl@ukr.net