УДК 004.9: 351.862.1

УПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРУ БЕЗПЕКИ

В.В. Бєгун, *канд. техн. наук*

Вступ. Інформаційні технології (ІТ) увійшли у сучасне життя людини майже в усіх сферах буття: ми не розлучаємося з мобільним телефоном, радимося з комп'ютером при виборі домашніх речей, отримуємо детальну інформацію з чека в супермаркеті. Але, на превеликий жаль, маємо протилежну ситуацію у сфері безпеки. Ми не знаємо, наприклад, яким повітрям дихаємо, навіть коли над містом стоїть густий смог. Не знаємо рівня безпеки продукції, будівельних матеріалів, які використовуються при ремонті шкіл, аж поки не починають тяжко хворіти діти. Це у побуті, а щодо техногенної безпеки ситуацію взагалі можна назвати критичною.

Аналіз досліджень і публікацій та постановка проблеми. Незважаючи на значний спад виробництва останніми роками, збитки від надзвичайних ситуацій (НС) значно збільшуються (рис. 1). Зростаючим є тренд кількості аварій і НС при невеликих зменшеннях (непропорційних до спаду виробництва) кількості постраждалих і загиблих. Знову ж таки, на превеликий жаль, у сфері безпеки та в побуті, у виробничій сфері Україна лідирує за кількістю постраждалих і загиблих на європейській частині континенту.

Причиною цього ганебного, на мій погляд, явища є застарілі методи управління безпекою із радянського минулого, а сучасні ІТ у цій сфері майже не використовуються.

Нещодавно у журналі «Вісник НАН України» була опублікована доповідь директора Інституту проблем математичних машин та систем (ІПММС) НАН України академіка А.О. Морозова на засіданні Президії НАН України 17 червня 2015 р. [1]. У його доповіді йшлося про причини відставання нашої держави від країн Європейського Союзу в упровадженні нових систем управління безпекою на основі принципів запобігання можливим техногенним аваріям і про першорядні завдання для профільних установ академії щодо переходу системи цивільного захисту в Україні до нової парадигми управління безпекою – так званого ризик-орієнтованого підходу (РОП) [1; 2]. Саме такого переходу вимагає Угода про асоціацію з Євросоюзом [3]. Крім того, про його необхідність свідчать результати досліджень учених, зокрема співробітників ІПММС НАН України [4–6].

Мета та задачі дослідження. Мета дослідження – проаналізувати розв'язання проблеми управління безпекою методом розробки інформаційної технології управління безпекою. Як задачі розглянемо:

– оцінки на основі статистичних даних різних сфер безпеки ефективності управління;

– аналіз структури управління безпекою на основі РОП і структури ІТБ й основних її складових на рівні об’єкта та галузі загалом;

– аналіз загальних вимог щодо програмного забезпечення та інтерфейсу програм.

Аналіз проблеми управління ризиком. У законі України [7] визначення ключового поняття «ризик» приводиться у його європейському розумінні, на відміну від раніше прийнятого у законодавстві, зокрема й Законі «Про об'єкти підвищеної небезпеки», а саме: «*ризик – кількісна міра небезпеки, що визначається функцією двох змінних – імовірності небажаної події й розміру збитку від неї*». Для цілей розрахунків вважають:

$$R = P \times U, \qquad (1)$$

де змінна P – це ймовірність аварії (небажаної події), а U – розмір її наслідків (збиток). Змінні P та U – складні випадкові функції багатьох змінних. Оскільки обидва співмножники в формулі (1) випадкові величини, то й ризик R є випадковою величиною. Ризик, що створюють об'єкти підвищеної небезпеки (ОПН), звичайно є неспадаючою випадковою функцією багатьох змінних [8] (рис. 2).

$$R = F(x1, x2, x3, x4, x5), \qquad (2)$$

де:

X1 – змінна урахування всіх імовірних сценаріїв аварій для всіх режимів роботи;

X2 – змінна, що враховує всі можливі вихідні події, природного характеру тощо;

X3 – змінна урахування зношеності основного обладнання та статистики його відмов;

X4 – змінна урахування типів захисного обладнання та його стану;

X5 – змінна урахування навченості персоналу.

Ризик, створений об'єктом, є суто індивідуальною характеристикою цього об'єкта. До того ж, ризик постійно змінюється [8], і лише завдяки реальним його оцінкам можливе ефективне управління на основі ризик-орієнтованого підходу. Як інтегральний показник захищеності Z вводиться індекс захищеності, визначений як відношення законодавчо встановленого допустимого значення інтегрального ризику для об'єктів певної групи R_d до поточного значення інтегрального ризику R_a:

$$Z = \frac{R_d}{R_a} \qquad (3)$$

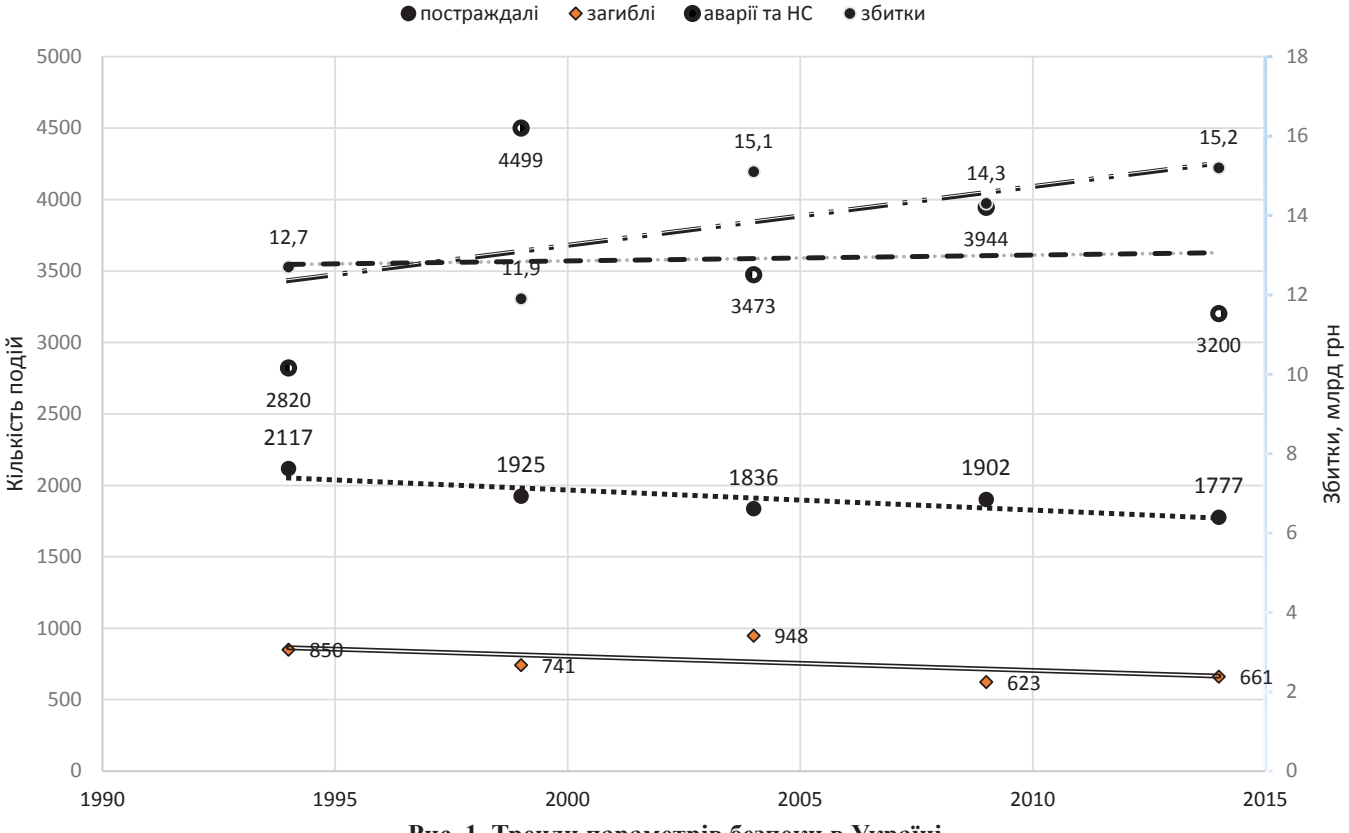


Рис. 1. Тренди параметрів безпеки в Україні

Законодавчо у нашій країні значення прийнятного ризику не встановлені. На рис. 1 наведено рівні, рекомендовані світовими товариствами ВООЗ й МООП: *незначний ризик – $R \leq 1 \cdot 10^{-6}$; припустимий ризик – $1 \cdot 10^{-6} \leq R \leq 5 \cdot 10^{-5}$; високий (терпимий) ризик – $5\ 10^{-5} \leq R \leq 5 \cdot 10^{-4}$; неприпустимий ризик – $R \geq 5 \cdot 10^{-4}$.*

На більш високий рівень ризику переходять з таких випадкових та невипадкових причин: старіння обладнання; деградація знань і вмінь персоналу; у разі інцидентів (деградації обладнання та неправильної його ідентифікації). Перехід з високого на більш низький рівень ризику можливий завдяки успішним поточним ремонтам, тобто заміні обладнання на надійніше, підвищенню кваліфікації персоналу або зміні персоналу на більш кваліфікований, іншим позитивним змінам у системі.

Отже, завдання контролю (моніторингу) безпеки має бути представлено як *алгоритм перевірки випадкової величини,* що є багатомірною функцією дійсних змінних. На жаль, чинні в Україні алгоритми контролю безпеки (ризику) відповідають застарілим нормам й прописані в підзаконних актах і наказах центральних органів влади (ЦОВ), в яких безпека об'єкта визначається на рівні експертного оцінювання стану певного обладнання та систем захисту. Виконання відомчих правил теж оцінюється людиною (інспектором), але навіть позитивна оцінка не надає інформації щодо рівня ризику. Це не відповідає новому законодавству, бо не враховуються реальні кількісні оцінки безпеки.

Звісно, потрібна розробка всіх атрибутів нової парадигми: методик визначення рівнів ризиків на базі сучасних наукових досягнень, створення відповідних моделей, алгоритмів і програмного забезпечення.

Нова технологія та нова структура управління безпекою, що пропонуються. Впровадження парадигми РОП неможливе без використання ІТ. У працях учених ІПММС [4–6; 8–9] визначено можливі шляхи наступних змін. Річ у тім, що потрібне не тільки впровадження інформаційних технологій, а й зміна структури управління безпекою. Тобто зміни повинні відбуватись одночасно, бо проблема багатогранна та має, принаймні, такі аспекти:

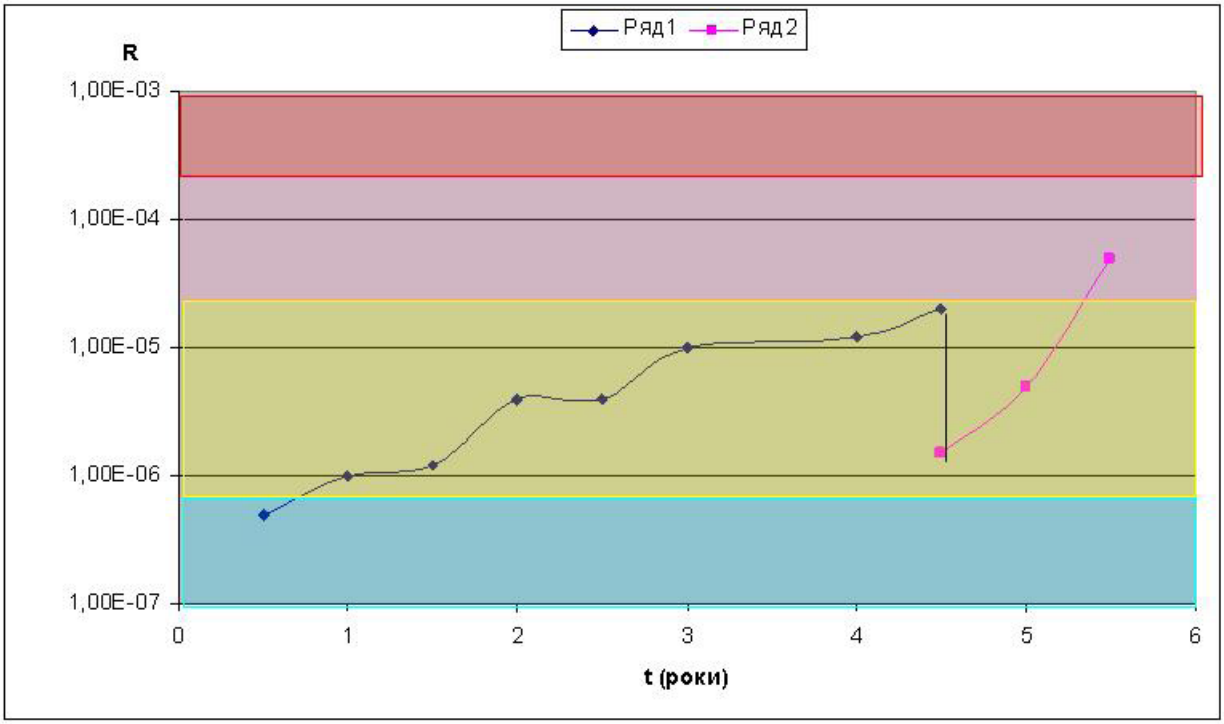


Рис. 2. Рівні ризику та можливі зміни ризику з часом

• політичний – потрібна дерегуляція управління, перевага повинна надаватися ринковим, економічним методам, а не інспекційним перевіркам;

• науковий – необхідно розробити нові методи, моделі, алгоритми, розрахункові програми (коди);

• інформаційний – потрібно впровадити інформаційну технологію;

• соціальний – стосується кожного громадянина.

Модель (структура) такого управління наведена на рис. 3.

Як бачимо, в структурі є тільки два елементи, що перебувають на бюджетному утриманні: органи державного нагляду за дотриманням чинного законодавства (істотно зменшені) та державні органи ліцензування експертів. Ці органи існують і в старій структурі, але тут їх функції змінені й, відповідно, чисельність зменшується в багато разів. Місцеві й державні органи влади контролюють тільки ступінь ризику R_a. Оскільки R_a є розрахунковою і випадковою величиною (2), стає зрозумілою необхідність впроваджувати інформаційні технології. Очевидно, порушувати питання управління ризиками доречно тільки за умови можливості обробки великого потоку інформації. Відповідна інформаційна технологія безпеки розроблена в ІПММС – її структура відображена на рис. 4. Розглянемо інформаційні задачі сучасної інформаційної технології управління ризиками, описаної нижче.

Ця інформаційна технологія дозволяє оператору приймати рішення і для вироблення заходів з метою запобігання неприйнятим рівням ризику, і для прийняття рішень після того, як аварія сталася. Інформаційну технологію в її прикладному застосуванні щодо безпеки позначимо як ІТБ. Формування структури комплексу інформаційних процесів з безпеки є одним із важливих етапів моделі ІТБ. На основі загальнотеоретичних знань і власного досвіду я визначив такі інформаційні процеси ІТБ:

ІП 1. Координація виконання інформаційних процесів.

ІП 2. Моніторинг і попередня обробка даних.

ІП 3. Оцінка рівня ризику.

ІП 4. Розпізнавання ситуацій.

ІП 5. Вироблення повідомлень і рекомендацій.

ІП 6. Виведення повідомлень і рекомендацій.

ІП 7. Корекція бази знань (БЗ) і бази даних (БД).

ІП 8. Збереження значень ознак та імені ситуацій.

Рис. 3. Структура органів управління безпекою за стратегією РОП

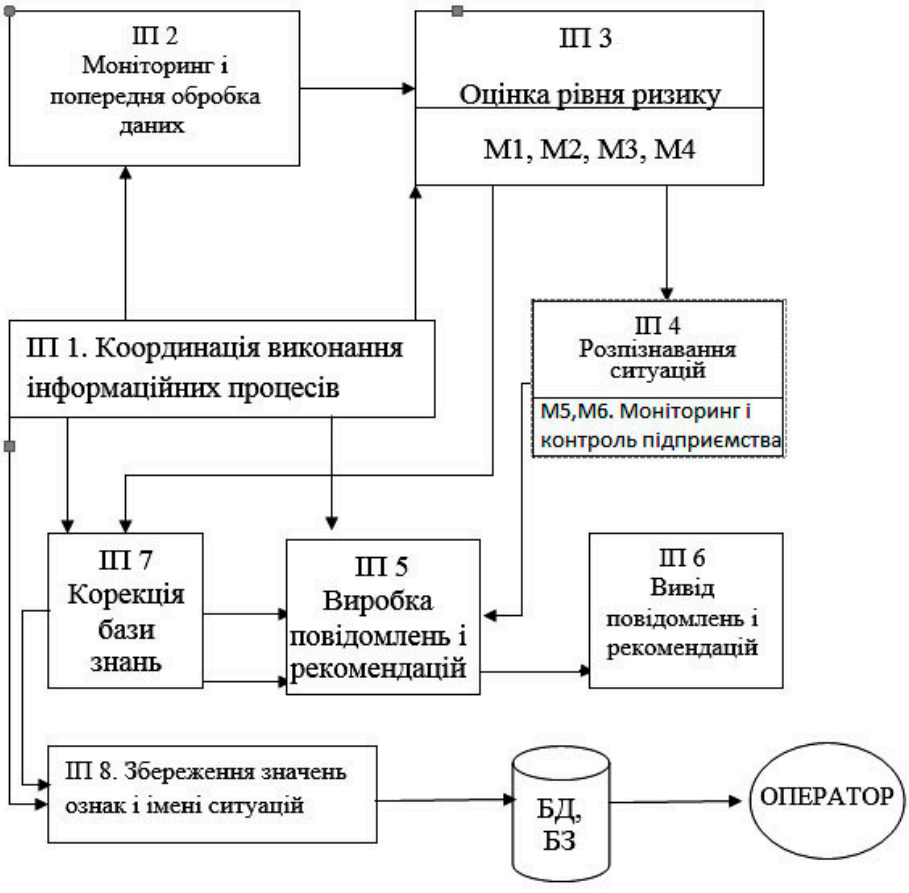


Рис. 4. Структура інформаційної технології безпеки

Функціонування цих процесів у системі управління безпекою утворює сучасну інформаційну систему безпеки. До основних функцій цієї системи віднесемо такі функції за нормальних (ФН) і аварійних умов (ФА) роботи:

ФА 1. Вироблення рекомендацій оператору при аваріях.

ФН 2. Вироблення рекомендацій щодо заміни обладнання, яке підвищує значення ризику за нормальних умов експлуатації.

ФН 3. Вироблення рекомендацій щодо зниження ризику.

ФН 4. Визначення поточних значень ризику та рівня культури безпеки.

ФН 5. Вироблення рекомендацій щодо визначення періоду перевірок.

ФН 6. Вироблення рекомендацій щодо підготовки персоналу.

ФН 7. Вироблення рекомендацій щодо страхування ризику.

Короткий опис цих функцій наведено у роботі [9]. У цій статті більшу увагу приділімо саме інформаційним задачам. Інформаційна технологія безпеки забезпечує автоматизацію управління безпекою як об'єктів, так і держави загалом. Отже, для виконання цих функцій необхідна розробка наступних математичних моделей:

М1. Типова модель галузі (для усіх небезпечних виробництв і процесів).

М2. Адаптована для підприємства (ОПН, блок АЕС) модель галузі.

М3. Модель визначення важливих базисних подій (БП).

М4. Модель визначення параметрів моніторингу.

М5. Модель моніторингу.

М6. Модель визначення параметрів БП.

М7. Моделі оцінок ризику: а) оцінка поточного значення ризику; б) оцінка стану безпеки.

М8. Модель вироблення рекомендацій щодо зниження ризику.

М9. Модель врахування можливих помилок персоналу.

М10. Модель розрахунків ризику персоналу на робочих місцях.

М11. Модель розрахунків ризику для населення регіону розміщення ОПН.

М12. Модель оцінок ризиків для сусідніх ОПН.

М13. Модель визначення рівня культури безпеки.

БД. Загальногалузева БД з безпеки.

Потрібно також визначити оптимальний (максимальний) проміжок часу між інспекціями T_m за умови врахування ризиків від усіх небезпек і неперевищення допустимого ризику:

$$Max\ (T_m): R_a < [R_d] \qquad (4)$$

Звісно, потрібна розробка відповідного програмного забезпечення (ПЗ). Дуже коротко вимоги до програмного забезпечення можна сформулювати так:

- сучасні мови програмування;
- інтуїтивно зрозумілий інтерфейс;
- лаконічний дизайн;
- вирішення завдань у реальному часі.

Опис, тим паче, розробка моделей і програмного забезпечення не є метою цієї статті, розглянемо дії з упровадження.

Необхідні зміни та можливості їх впровадження. Підсумовуючи все, можна сказати, що для реалізації нових принципів управління безпекою (РОП) нашої держави насамперед необхідно:

- виконати рекомендації щодо структури ЦОВ з безпеки;
- розробити моделі ІТБ для різних небезпек і галузей виробництва;
- розробити національну БД;
- розробити методики і керівництва з контролю за інформаційними процесами;
- змінити законодавство та НД;
- розробити моделі актуарних розрахунків;
- створити програмне забезпечення;
- змінити програми освіти з безпеки.

Це першочергові завдання. Довгострокові завдання впровадження РОП, ІТ та підвищення безпеки наступні:

- принциповий перехід на більш високі рівні та парадигми безпеки;
- зміни ідеології суспільства щодо безпеки;
- контроль інтегральних рівнів безпеки;
- інтеграція у міжнародні системи.

Висновки

Перехід на нову парадигму управління безпекою в Україні очевидно потрібен і здійснити його можна досить швидко. Наукові основи впровадження ризик-орієнтованого підходу в управлінні техногенно-екологічною безпекою, зважаючи на її високе значення як для кожного підприємства, так і для держави загалом, повинні мати найвищій пріоритет у суспільстві. НАН України має займатися розробленням математичних моделей і програмного забезпечення, центральні органи влади та суб'єкти господарювання – створенням відповідних структур управління безпекою і реорганізацією старих, впровадженням нових методів управління та ситуаційних центрів. Успіх залежить від ефективної взаємодії та координації робіт, передбачених планом заходів щодо реалізації Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Морозов А.О.* Наукові основи впровадження ризик-орієнтованого підходу в управлінні техногенно-екологічною безпекою / *А.О. Морозов* // Вісник НАН України. – 2015. – № 8. – С. 24–32.

2. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру [Електрон. ресурс]: Розпорядження Кабінету Міністрів України від 22.01.2014 № 37-р. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/37-2014-%D1%80

3. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електрон. ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/984_011

4. *Белов П.Г.* Теоретические основы менеджмента техногенного риска : дис. … д-ра техн. наук : 05.26.03 / *П.Г. Белов.* – Москва, 2007. – С. 33.

5. *Бегун В.В.* Решение задачи определения текущего уровня риска (мониторинга) с применением алгоритмов

МГУА. Моделирование-2012 / *В.В. Бегун, В.В. Литвинов* : Матер. конф. – К. : ІПМЕ ім. Г.Е. Пухова, 2012. – С. 92–96.

6. *Гречанінов В.Ф.* Інформаційні технології аналізу стану техногенної безпеки та планування протидії надзвичайним ситуаціям: дис. … канд. техн. наук : 05.13.06 / *В.Ф. Гречанінов.* – К., 2014. – С. 20.

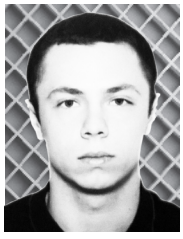
7. Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності». – № 877-V. – 5.04.2007 р.

8. *Бегун В.В.* Мониторинг риска объектов повышенной опасности на основе предварительного моделирования / *В.В. Бегун* : Зб. наук. праць «Моделювання та інформаційні технології» Міжнар. наукового семінару «Моделювання-2010». – К. : ІПМЕ ім. Г.Є. Пухова, 2010. – Т.1. – С. 152–163.

9. *Гречанінов В.Ф.* Актуальні проблеми моделювання ризиків і загроз критичних інфраструктур. / *В.Ф. Гречанінов, В.В. Бєгун, В.П. Клименко, О.П. Яцук* // Науковий вісник Укр.НДІПБ. – 2015. – № 1. – С. 125–134.

УДК 681. 335 (088.8)

ПРИСТРІЙ ДЛЯ ЛІНЕАРИЗАЦІЇ НЕЛІНІЙНИХ ХАРАКТЕРИСТИК



О.Й. Рішан,
канд. техн. наук,
В.С. Денисенко

Постановка проблеми. При перетворенні аналогових сигналів первинних вимірювальних перетворювачів (**ПВП**) у цифровий код, з подальшою їх обробкою у мікропроцесорних контролерах комп'ютерно-інтегрованих систем керування технологічними процесами, доцільно в якості проміжного перетворювача використовувати конденсаторний перетворювач напруги у частоту, побудований за схемою транзисторного **RC**-генератора [2]. Такий генератор забезпечує пропорційне перетворення аналогового вихідного сигналу **ПВП** по напрузі у частоту його релаксації по трьом незалежним каналам: зміни швидкості заряду ємностей **RC**-генератора за рахунок зміни їх струму заряду по емітерним і базовим ланцюгам стабілізаторів струму та регулювання рівня заряду ємностей по напрузі [1]. Водночас генератор забезпечує глибоке регулювання частоти його релаксації по цим каналам аналоговими вихідними сигналами від операційних підсилювачів, які обробляють сигнали **ПВП** до їх перетворення в частоту, оскільки живлення самого **RC**-генератора здійснюється напругою живлення операційних підсилювачів.

У разі одночасного використовування перших двох каналів регулювання частоти **RC**-генератора за рахунок зміни струму заряду його ємностей по емітерним і базовим ланцюгам стабілізаторів струму можна здійснювати алгебраїчне додавання двох сигналів по цим входам за основним рівнянням його перетворення у вигляді:

$$F(h) = F_0 + a * [\pm f(h) \mp \varphi(h)], \qquad (1)$$

де $F(h)$ – частота імпульсів на виході генератора; F_0 – початкова частота релаксації **RC**-генератора; a – коефіцієнт перетворення **RC**-генератора; $f(h)$ – сигнал **ПВП**, який підлягає перетворенню у частоту імпульсів; $\varphi(h)$ – сигнал коригування характеристики перетворення **ПВП** для зменшення її нелінійності; h – фізичний параметр, який перетворюється у частотний сигнал.

Залежність (1) дає можливість реалізувати спосіб лінеаризації і побудувати на основі **RC**-генератора пристрій для лінеаризації аналогового сигналу **ПВП** із гармонічною характеристикою перетворення (**ХП**).