ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 658.012.4:621 doi.org/10.33298/2226-8553.2025.2.43.20

© Тупкало В.М., Богом'я В.І., Ярмолатій А.В.

КОНЦЕПТУАЛЬНІ ЗАСАДИ СИСТЕМОТЕХНІКИ КІБЕРЗАХИЩЕНИХ ЦИФРОВИХ СИСТЕМ НА ОСНОВІ ВИКОРИСТАННЯ АПАРАТУ СИНТЕЗУ СИГНАТУРНОЇ АЛГЕБРИ

Гарантування безпеки та стійкості національної критичної інфраструктури сьогодні є пріоритетним напрямком безпекової політики України, оскільки критична інфраструктура забезпечує життєвоважливі для населення, суспільства та держави, без яких неможливо безпечне існування та забезпечення належного рівня національної безпеки. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах нашого життя та, відповідно, до зросту уразливостей і потенційних загроз різного характеру. Очевидно, що за таких умов забезпечення кібертехнологій у критичних інфраструктурах (інфраструктурах державного управління, фінансового, банківського, транспортного, енергетичного, ресурсного, комунального та продуктового забезпечення) сучасного суспільства стає одним з головних питань.

В контексті необхідності рішення комплексної проблеми забезпечення кіберстійкості цифрових систем управління критичної інфраструктури запропонований новий сигнатурний логіко-поліноміальний підхід до синтезу апаратної надмірності функціонального у реальному масштабі часу контролю арифметичних та логічних операцій цифрових систем, який зводиться до побудови апаратної надмірності комбінаційного типу. Синтез ґрунтується на математичному апараті авторської сигнатурної логіко-поліноміальної алгебри поля TSF[2^n, $P^m(x)$].

***Ключові слова**: кіберстійкість, критична інфраструктура, інформаційна безпека, методи функціонального контролю цифрових систем.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сьогодні існує декілька напрямків рішення комплексної проблеми забезпечення інформаційної безпеки функціонування цифрових, систем критичної інфраструктури (ЦСКІ), наприклад, шляхом використання методів багаторазового резервування баз даних, резервування апаратних частин цифрових систем і систем в цілому, введення різноманітної інформаційної надлишковості в програмне забезпечення та у процес передачі цифрових даних. З цього приводу слід зазначити, що при побудові математичних моделей функціонального контролю складних систем, до яких відносяться ЦСКІ, неминучим є ряд проблем. Зокрема, ці моделі пов'язані з наявністю асинхронних паралельних процесів, численних внутрішніх зав'язків між елементами системи, великої кількості її параметрів, різноманітних нелінійних обмежень. Тому застосування наведених вище методів для аналізу характеристик контролю таких систем призводить до суттєвого спрощення реальних процесів і, як наслідок, ставить під сумнів адекватність розробленої моделі функціонального контролю за цими методами щодо синтезу ефективних систем оперативного моніторингу стану інформаційної безпеки (кібербезпеки). Виходячи з цього, в першу чергу, актуальної у теоретичному і практичному сенсі стає пошук нового системотехнічного підходу до синтезу кіберзахищених цифрових систем критичної інфраструктури на основі дослідження механізму функціонального (оперативного у часі) контролю

реалізації арифметичних і логічних операцій над двійковими числами (операндами) на єдиній методологічній основі.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання проблеми функціонального контролю і на які спирається автор.

Сьогодні одним із факторів стримування розвитку ефективних методів функціонального (у реальному часі) контролю (ФК) цифрових автоматів є подальше прагнення вибору та обґрунтування моделі ФК шляхом введення апаратної надмірності у вигляді багаторазового дублювання (резервування) ЦА [1]) та інформаційної (кодової) надмірності [2]. Істотним недоліком такого введення інформаційної (кодової) надмірності для кожного двійкового коду є залежність контрольного коду від кратності прояву помилок (ступеню спотворення інформації). Тому найбільш поширеним методом ФК різних типових пристроїв обчислювальної техніки та цифрових керуючих автоматів є **контроль парності-непарності коду двійкового числа (додавання до значущих розрядів кодів чисел не більше одного контрольного розряду). Цей метод ФК не забезпечує виявлення кратних помилок [3].**

В контексті визначеної проблеми забезпечення ефективного ФК цифрових систем різного призначення відомий ряд робіт [4-11], в яких розглянуті питання вибору моделей апаратного контролю шляхом введення апаратної надмірності (надлишковості). Як правило, кожний автор (автори) формують свою задачу дослідження ФК відносно розгляду окремого конкретного типу та призначення цифрового пристрою. При цьому не враховується, що ці пристрої по своєму функціональному призначенню можуть знаходитись у нерозривному системному єднанні апаратних та програмних засобів цифрових систем відповідного цільового призначення.

Мета статті. Обґрунтування та формування пропозиції щодо подальшого напрямку розвитку системотехніки кіберзахищених ЦСКІ шляхом введення уніфікованої структурної (апаратної) надмірності ФК комбінаційного (булевого) типу на основі використання авторського апарату синтезу «сигнатурна логіко-поліномійна алгебра» [12] .

Виклад основного матеріалу дослідження. Відомо, що єдиною методологічною (системотехнічною) основою всіх арифметичних операцій в цифрових системах є елементарні операції додавання та регістрового зсуву [13]. При цьому слід зауважити, що регістрова операція зсуву знижує швидкість виконання арифметичних операцій. Тому, в контексті сформульованої вище загальної проблеми, пропонується моделі абстракції синтезу апаратурної надмірності для функціонального контролю обраних операцій (арифметичних так і булевих логічних) ЦСКІ визначити відповідними (адекватними) їм описами у інфіксній нотації (інфіксними моделями). у вигляді детермінованих контрольних арифметичних функцій. Правомірність такої пропозиції виходить з тенденції розвитку сучасних ЦСКІ на принципах глибокої уніфікації, стандартизації структур сигналів та інтерфейсів.

Постановка задачі. Згідно поставленої мети пропонується наступне визначення.

Визначення 1. Функціональна кіберконтролепридатність цифрової інформаційно-вимірювальної системи комплексу управління об’єктом критичної інфраструктури — це властивість системи, яка характеризує придатність частини або всіх властивих їй виконуваних цільових обчислювальних операцій $f_i \in F(X_{[n]})$ над n-розрядними операндами $X_{[n]}$ до виявлення заданими засобами функціонального контролю хакерських втручань (інцидентів) в процесі виконання функцій f_i у реальному масштабі часу.

В контексті сутності визначення 1 модель функціонального контролю ЦСКІ представлена на рис. 1.

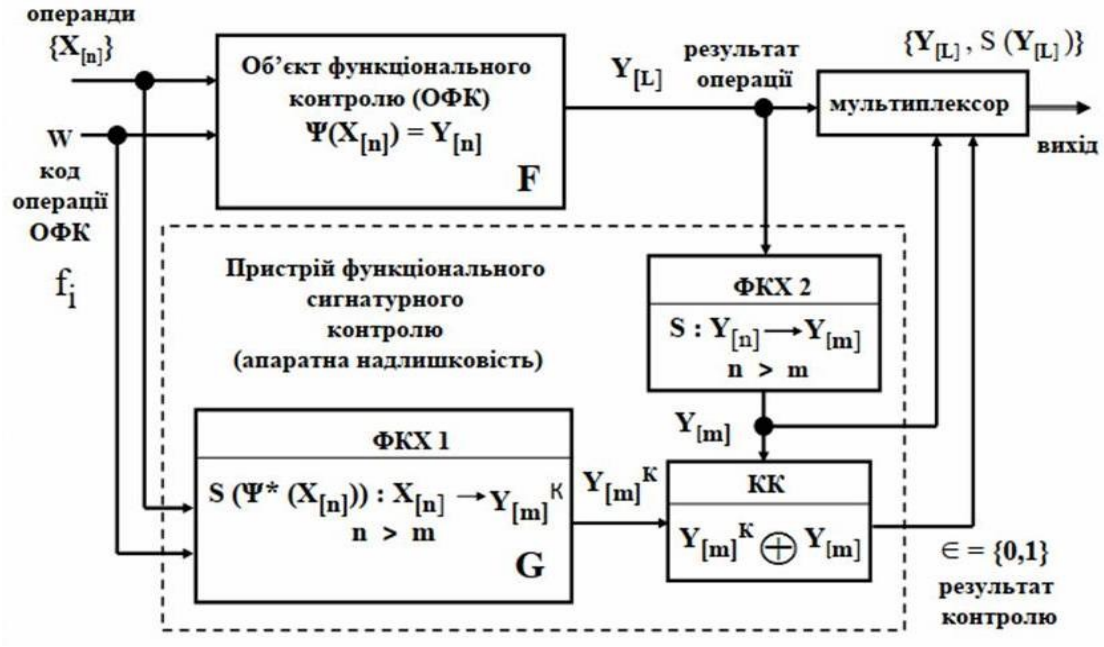

Рисунок 1 – Модель функціонального контролю (авторська модель)

Щодо цієї моделі: об'єкт функціонального контролю (ОФК) — цифровий автомат (арифметико-логічний модуль ЦСКІ) з передавальною функцією Ψ; пристрій контролю складається з трьох комбінаційних схем (апаратна надмірність), який в залежності від виду контрольованої функції f_i здійснює формувачем контрольних характеристик ФКХ 1 сюр'єктивне відображення:

$$S(\Psi^*(X_{[n]})) : X_{[n]} \rightarrow Y_{[m]}^K \qquad (1)$$

вхідних двійкових векторів $X_{[n]}$ довжини n у вихідні двійкові вектори $Y_{[m]}^K$ довжини m (n > m) відповідно до повідомлених йому від ОФК іменами (кодами) f_i контрольованих операцій з множини F; здійснює формувачем контрольних характеристик ФКХ 2 сюр'єктивне відображення:

$$S: Y_{[n]} \rightarrow Y_{[m]} \qquad (2)$$

вхідних двійкових векторів $Y_{[n]}$ довжини n у вихідні двійкові вектори $Y_{[m]}$ довжини m; оператор S необхідний для кодування векторів довжини n у відповідні їм вектори довжини m, щоб забезпечувалася задана достовірність функціонального контролю; компаратор m — розрядних кодів (КК) здійснює відображення:

$$\delta_{KK} : (Y_{[m]}^K \oplus Y_{[m]}) \rightarrow \in = \{0,1\} \qquad (3)$$

шляхом ідентифікації відповідності кожного вектора виходу ОФК $y_i \in Y_{[m]}$ з відповідними векторами $y_{ki} \in Y_{[m]}^K$.

Згідно встановленим вище вимогам пошуку стандартного набору комбінаційних елементів для синтезу ВК залежність між функціями $\Psi(X_{[n]})$ та $\Psi^*(X_{[n]})$ визначимо у інфіксному вигляді (нотації):

$$\Psi(X_{[n]}) = \Psi^*(X_{[n]}) = (\psi_1 * \psi_2 * \cdots * \psi_q), \qquad (4)$$

де * та ψ_j — відповідно логічна операція суперпозиції (комутації) та j-та елементарна логічна складова універсального представлення логіко-поліноміальним еквівалентом множини F цільових контролюємих арифметичних та логічних операцій ЦСКІ.

Виходячи з вищезазначеного, сутність задачі забезпечення функціональної кіберконтролепридатності ЦСКІ визначимо так: нехай для заданого ОФК доступними для контролю є його входи

та виходи. Треба знайти для цього ОФК опис множини контрольних характеристик G для всіх можливих виконуваних ОФК операцій множини F з метою подальшого синтезу ФКХ 1 у вигляді такому, щоб контрольовані функції $\Psi(X_{[n]})$ множини F були представлені відповідною еквівалентною логічною функцією (4), а оператор S був би таким, щоб допускалося сюр'єктивне відображення згідно принципу суперпозиції:

$$S(\Psi(X_{[n]})) = S(\Psi^*(X_{[n]})) = S\psi_1 * S\psi_2 * \cdots * S\psi_q . \quad (5)$$

Основний результат. В основу рішення задачі синтезу (5) покладено математичний апарат авторської сигнатурної логіко-поліноміальної алгебри, яка має наступне визначення [14].

Визначення 2. Сигнатурна логіко-поліноміальна алгебра — це алгебра сюр'єктивного відображення над кінцевим полем двійкових чисел Tupkalo Signature Field TSF $[2^n, P^m(x)]$ довжини *n* у сигнатури (sig) довжиною

m (*n* > *m)*, множиною алгебри поля є системна множина:

$$W = (R; \oplus, H, H^1, sig, \alpha, \beta, \varphi), \quad (6)$$

де, R – множина арифметичних та логічних функції ЦІВС, які обрані об'єктами функціонального (оперативного у часі)) контролю;

дві бінарні логічні операції: складання за модулем два та логічна операція формування взаємної поліноміальної характеристики (H*)* двох чисел, які вступають в операцію арифметичного складання;

дві унарні операції: операція однорозрядного усікання лівого старшого розряду числа взаємної поліноміальної характеристики (H^1), якщо це вимагає умова виконання певної контрольованої арифметичної операції над парою двійкових чисел в контексті моделі (6); операція комбінаційного типу формування сигнатури (sig) двійкового числа;

три *n* - розрядні константи*: φ* — двійкове число з одиницею тільки у молодшому розряді, *α* — двійкове число з одиницями у всіх розрядах (константа інвертування), *β* — двійкове число з одиницею тільки у старшому розряді.

Твердження 1. Детермінованій арифметичній функції Ψ(X) може бути поставлено у відповідність S-перетворення її логіко-поліномного еквіваленту у інфіксному вигляді (5), якщо кожна з функцій ψ_j є унарною або бінарною, оператор S є лінійним, а операція $*$ є складання за модулем два .

Доказ твердження 1. Оскільки умовою виконання рівності (2) є незалежність вибору оператора S від функції Ψ*(X), то існування для детермінованої арифметичної функції Ψ(X) її булевого еквіваленту в принципі не виключає її інфіксного представлення (1). У свою чергу, оскільки розглядається безперервний у часі (безперервний за тактами роботи (тактовим моментам) цифрової системи) контроль, то з рішення 13-ї проблеми Гільберта відомо, що будь-яка безперервна функція N змінних представима як суперпозиція безперервних функцій двох змінних [15]. Тоді принцип суперпозиції (2) реалізується, якщо має місце лінійне S-перетворення лінійної булевої функції. Лінійність булевого еквівалента (5) можлива в тому випадку, коли всі функції ψ_j є функціями однієї та (або) двох змінних за умови представлення ψ_j та $*$ сумою за модулем два або еквівалентністю [16].

Припустимо, що S – несюр'єктивне відображення. Тоді повинен бути хоч би один такий вектор $y_j^K \in Y_{[m]}^K$ на вході компаратора КК (див. рис.1), що для всіх x_j на вході ФКХ 1 $S(x_j) \neq y_j^K$. Проте перехід безпомилково працюючого ФКХ 1 в працездатний стан з таким y_j^K суперечить сутності організації функціонального (аппаратного) контролю:

$$S(\Psi^*(X_{[n]})) : X_{[n]} \rightarrow Y_{[m]}^K$$

і тому є сюр'єктивним відображенням, що й потрібно було довести.

З урахуванням твердження 1 логіко-поліноміальний еквівалент арифметичної функції складання $F^{(+)}$ має вигляд:

$$A + B = (A \oplus B) \oplus H(A + B) = A \oplus B \oplus H(A + B), \quad (7)$$

де, H (A + B) – число, код якого характеризує перехід одиниць перенесення при операції складанні чисел A і B. Оскільки H(A+B) встановлює по суті взаємний поліноміальний зв'язок між числами A і B, то в сигнатурній алгебрі H (A+B) визначено як взаємну поліноміальну характеристику двох чисел, які вступають в операцію арифметичного складання.

Приклад 1. A = 1011011, B = 0111011.

$$H(A+B) = \begin{pmatrix} 1\,0\,1\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0\,1\,1 \end{pmatrix} = 1\,1\,1\,1\,0\,1\,1\,0$$

$$A + B = \begin{pmatrix} 1011011 \\ 0111011 \\ 11110110 \end{pmatrix} \oplus = 10010110$$

Слід зауважити, якщо операнди A і B операції арифметичного складання описуються поліномами n-го ступеню, а їх характеристика H(A+B) може описуватися поліномом (n + 1) ступеню. При цьому задача синтезу формувача характеристики H(A+B) зводиться до побудови комбінаційного (булевого) вузла, який реалізує на своїх виходах систему булевих функцій:

$$\begin{cases} h_1 = 0; \\ h_2 = a_1 b_1; \\ h_{i>2} = h_{i-1}(a_{i-1} \vee b_{i-1}). \quad i = 3, \cdots, n+1. \end{cases} \qquad (8)$$

В контексті твердження 1 відносно вимоги щодо лінійності оператора S слід зазначити наступне. В роботі [6] показано, що цей оператор може бути лінійним у разі його векторної інтерпретації (sig) як унарної операції сюр'єктивної згортки двійкового числа A довжини *n* у його контрольну характеристику (сигнатуру) довжини *m* по модулю незвідного примітивного полінома $P^m(x)$ ступеню *m* при умові дотримання співвідношення $n = (2^m - 1)$. Тобто, сигнатура числа $A_{[n]}$ є сюр'єктивним відображенням:

$$sigA_{[n]} = A_{[n]} \bmod P^m(x). \qquad (9)$$

Виходячи з цього, у разі логіко-поліноміального еквіваленту арифметичної функції складання $F^{(+)}$ (7) суперпозиційна формула (алгоритм) функціонального сигнатурного контролю операції арифметичного складання двійкових операндів має вигляд:

$$sig\,(A + B) = sig\,A \oplus sig\,B \oplus sig\,H\,(A + B). \qquad (10)$$

Слід зауважити, що у разі, коли розрядність операндів *n* значно перевищує ступінь *m* полінома формування сигнатур, запропонований авторський метод коректного рішення цієї ситуації - блоково-композиційний метод формування контрольних сигнатур функціонування цифрових систем на основі властивостей сигнатурного поля $TSF[2^n, P^m(x)]$ (Tupkalo signature field) [17, 18].

З вищезазначеного, в контексті моделей (7) і (10) доказано:

1. Оскільки операція арифметичного складання двійкових чисел є основою операцій віднімання, множення і ділення двійкових чисел, то результат любої арифметичної функції (операції) може бути представлений її логіко - комбінаційним еквівалентом і, як слідство, – сигнатурним поліномом (права частина рівняння (10)) згідно визначенню: *сигнатурна формула у вигляді суми по модулю два сигнатур називається сигнатурним поліномом, якщо хоча б одна з сигнатур пов'язана з взаємною поліноміальною характеристикою двох операндів* H[A + B].

2. Алгоритм функціонального сигнатурного контролю любої бінарної двійкової логічної операції в функціонально повній системі логіко-поліноміальної сигнатурної алгебри В.Тупкало може бути представлений як *сигнатурний поліном.*

Висновки. Наукова новизна отриманих теоретичних результатів по суті закладає новітній напрямок системології розвитку цифрових систем критичної інфраструктури - функціональний сигнатурний контроль цифрових систем шляхом введення в об'єкти контролю уніфікованої структурної (апаратної) надмірності комбінаційного (булевого) типу на основі використання апарату синтезу «сигнатурна логіко-поліномійна алгебра поля $TSF[2^n, P^m(x)]$».

ЛІТЕРАТУРА

1. Методи підвищення надійності. Основні поняття та види резервів. URL: Резервування.pdf (ztu.edu.ua) (дата звернення: 14.03.2025)
2. Блейхут Р. 1986 Теорія и практика кодов, контролирующих ошибки. Мир. 576 с.
3. Ашаріна И. В. Проблеми організації обчислювань в багатомашинних обчислювальних системах з програмно-керуємою збої та відмовостійкістю, 2021.Частина І. АТ «НДІ«Субмікрон».20 с.
4. Контроль роботи цифрового автомату. Систематичі коды. URL: https://koralexand.ua/?page_id=129 (дата звернення: 15.03.2025)
5. Застосування контролю інформаційних слів та їх адрес по mod 3 в цифрових пристроїв автоматики. URL: https://works.doklad.ru/view/MWsnskSFwF8/all.html (дата звернення: 15.03.2025)
6. Якимець Н., Харченко В. Відмовостійкі цифрові системи управління з програмованою логікою на основі частково працездатних автоматів: моделі та реалізація. НАУ ім. Н.Є. Жуковського, "ХАІ". Системи бробки інформації. Випуск 4 (62), 2007. С. 134-138.
7. Федухін А., Сеспедес Гарсія П. До питання про структури стійких до відмов комп'ютерів фірми stratus computer inc. Математичні машини та системи. № 4, 2018. С. 87-100.
8. Методи апаратурного контролю. URL: https://studfile.net/preview/9099982/page:17/ (дата звернення: 10.03.2025)
9. Програмно-логічні методи контролю. URL:https://studfile.net/preview/9099982/page:18/ (дата звернення: 10.03.2025)
10. Числовий та цифровий контроль. URL: https://studfile.net/preview/4354159/page:15/ (дата звернення: 10.03.2025)
11. Окремі випадки контролю за модулем. Способи побудови схем згорток. URL: https://studfile.net/preview/4354159/page:16/ (дата звернення: 12.03.2025)
12. Тупкало В.М. Розробка моделей кіберстійких інформаційних систем управління на основі використання математичного апарату сигнатурної алгебри: *авторське свідоцтво* № 131020; заяв. 31.10.2024; опубл. 29.11.2024, Бюл. № 84.
13. Самофалов К., Корнейчук В., Романкевич А. Прикладна теорія цифровых автоматів. Київ: Вища шк. Головне вид-во, 1987. 375 с.
14. Тупкало В.М. Розробка моделей кіберстійких інформаційних систем управління на основі використання математичного апарату сигнатурної алгебри. V Міжнарод. наук.-практ. конф. «Управління якістю в освіті та промисловості: досвід, проблеми та перспективи»,. зб. тез доп. Львів: ЛА «Піраміда», 2021. С. 186-187.
15. Вітушкін А.Г. 2004 13-а проблема Гільберта та суміжні питання. УМН. Т. 59, № 1(355), 2004. С. 11–24.
16. Тупкало В.М. Основи теорії сигнатурного контроля цифрових систем: монографія. МінОборони України, 1994. 324 с.
17. Тупкало В.М. Блоково-композиційний метод формування контрольних сигнатур функціонування цифрових систем на основі властивостей сигнатурного поля TSF[2^n, $P^m(x)$]: авторське свідоцтво № 133106. Дата реєстрації 04.03.2025..
18. Tupkalo V. Block-composition method of forming control signatures of digital systems operation based on the properties of the signature field TSF[2^n,$P^m(X)$]. Information Technology: Computer Science, Software Engineering and Cyber Security. № 4, 2024. P. 206-215.

REFERENCES

1. Methods for increasing reliability. Basic concepts and types of reserves. URL: Reserve.pdf (ztu.edu.ua) (access date: 14.03.2025)
2. Bleikhut R. 1986 Theory and practice of error-controlling codes.Mir. 576 p.
3. Asharina I. V. Problems of organizing calculations in multi-machine computing systems with software-controlled failure and fault tolerance, 2021. Part I. JSC «NDI» Submicron. 20 p.

4. Control of the operation of a digital automaton. Systematic codes. URL: https://koralexand.ua/?page_id=129 (access date: 15.03.2025)
5. Application of control of information words and their addresses by mod 3 in digital automation devices. URL: https://works.doklad.ru/view/MWsnskSFwF8/all.html (access date: 15.03.2025)
6. Yakimets N., Kharchenko V. Fault-tolerant digital control systems with programmable logic based on partially operational automata: models and implementation. NAU named after N.E. Zhukovsky, "KHAI". Information processing systems. Issue 4 (62), 2007. P. 134-138.
7. Fedukhin A., Cespedes Garcia P. On the question of structures of fault-tolerant computers of the company stratus computer inc. Mathematical machines and systems. No. 4, 2018. Pp. 87-100.
8. Methods of hardware control. URL: https://studfile.net/preview/9099982/page:17/ (date of access: 10.03.2025)
9. Software-logical control methods. URL: https://studfile.net/preview/9099982/page:18/ (date of access: 10.03.2025)
10. Numerical and digital control.URL: https://studfile.net/preview/4354159/page:15/ (date of access: 10.03.2025)
11. Certain cases of control by module. Methods of constructing schemes convolutions. URL:https://studfile.net/preview/4354159/page:16/ (date of access: 12.03.2025)
12. Tupkalo V.M. Development of models of cyber-resistant information systems management based on the use of mathematical apparatus of signature algebra: author's certificate №. 131020; application. 31.10.2024; publ. 29.11.2024, Bull. No. 84.
13. Samofalov K., Korneychuk V., Romankevych A. Applied theory of digital automata. Kyiv: Higher school. Main publishing house, 1987. 375 p.
14. Tupkalo V.M. Development of models of cyber-resistant information systems management based on the use of mathematical apparatus of signature algebra. V International scientific and practical conference Quality management in education and industry: experience, problems and prospects",.collection of abstracts of additional Lviv: LA "Pyramid", 2021. P. 186-187.
15. Vitushkin A.G. 2004 Hilbert's 13th problem and related issues. Uspekhi Mater. Vol. 59, No. 1(355), 2004. P. 11–24.
16. Tupkalo V.M. Fundamentals of the theory of signature control of digital systems: monograph. Ministry of Defense of Ukraine, 1994. 324 p.
17. Tupkalo V.M. Block-composition method for forming control signatures of the functioning of digital systems based on properties of the signature field TSF[2n, Pm(x)]: author's certificate №. 133106. Registration date 04.03.2025.
18. Tupkalo V. Block-composition method of forming control signatures of digital systems operation based on the properties of the signature field TSF[2n,Pm(X)]. Information Technology: Computer Science, Software Engineering and Cyber Security. No. 4, 2024. R. 206-215.

Tupkalo V.M., Bogomya V. I., Yarmolatiy A. V.

CONCEPTUAL BASIS OF SYSTEMS ENGINEERING OF CYBER-PROTECTED DIGITAL SYSTEMS BASED ON THE USE OF THE APPARATUS FOR SYNTHESIS OF SIGNATURE ALGEBRA

Ensuring the security and sustainability of national critical infrastructure is a priority area of security policy today, since critical infrastructure provides vital services for the population, society and the state, without which safe existence and ensuring an adequate level of national security are impossible. The main reasons for the criticality of the information component of the infrastructure stem from the rapid spread of information technologies in all areas of our lives and, accordingly, the growth of vulnerabilities and potential threats of various kinds. It is obvious that in such conditions, ensuring cyber technologies in critical infrastructures (infrastructures of public administration, financial, banking, transport, energy, resource, utilities and food supply) of modern society is becoming one of the main issues.

In the context of the need to solve the complex problem of ensuring cyber resilience of digital control systems of critical infrastructure, a new signature logical-polynomial approach to the synthesis of functional hardware redundancy in real time for monitoring arithmetic and logical operations of digital systems is proposed, which is reduced to the construction of hardware redundancy of a combinational type. The synthesis is based on the mathematical apparatus of the author's signature logical-polynomial algebra of the TSF[2n, Pm(x)] field.

Keywords: *cyber resilience, critical infrastructure, information security, methods of functional control of digital systems.*

Стаття прийнята 20.03.2025