



**ЛЕТИЧЕВСЬКИЙ**  
**Олександр Олександрович** — доктор фізико-математичних наук, завідувач відділу теорії цифрових автоматів Інституту кібернетики ім. В.М. Глушкова НАН України

## АЛГЕБРАЇЧНЕ МОДЕЛЮВАННЯ ТА ЙОГО ЗАСТОСУВАННЯ

*Статтю присвячено науковим розробкам Інституту кібернетики ім. В.М. Глушкова НАН України, пов'язаним із застосуванням технологій алгебраїчного та інсерційного моделювання на основі алгебри поведінок. Розглянуто технології формалізації, алгебраїчної верифікації та тестування програмних і апаратних специфікацій у рамках модельного способу розроблення програмних систем. Приділено увагу використанню алгебраїчного моделювання в біологічних дослідженнях, створенні систем на основі блокчейн-платформ, аналізі правових та економічних моделей. Як один з основних напрямів практичного застосування зазначених технологій виокремлено галузь кібербезпеки, в якій використовується метод алгебраїчного зіставлення та формалізація шаблонів вразливостей і кібератак.*

**Ключові слова:** алгебраїчне моделювання, вразливості коду, модельний метод розроблення, інсерційне моделювання, формальна верифікація, модельне тестування, гібридні інтелектуальні системи.

У 70-х роках минулого століття у відділі теорії цифрових автоматів, яким керував засновник Інституту кібернетики академік Віктор Михайлович Глушков, було розроблено одну з перших у світі систем автоматичного доведення теорем [1], що поклало початок розвитку технології алгебраїчного програмування. Систему APS (Algebraic Programming System) [2] було створено як інструментарій для реалізації алгебраїчних алгоритмів з метою автоматичного доведення тверджень, розв'язання рівнянь у різних теоріях, задач доказового програмування, паралельного програмування, перетворень формальних специфікацій та інших проблем.

Перші програми символічного моделювання було написано мовою АПЛАН, що ґрунтується на застосуванні систем переписувальних правил. Надалі цей напрям активно розвивався, оскільки символічне моделювання виявилось ефективним для вирішення багатьох індустріальних завдань у різноманітних предметних галузях. Продовженням алгебраїчного програмування стала технологія інсерційного моделювання [3]. Вона узагальнювала алгебраїчний підхід для формалізації процесів, які можна описувати як взаємодію агентів та їх занурення (insertion) у середовище.

Уперше систему інсерційного моделювання було впроваджено на практиці для вирішення завдань, пов'язаних з верифікацією та тестуванням телекомунікаційних систем та їхніх програмних і апаратних компонентів. З 2000 р. розпочалася активна співпраця Інституту кібернетики ім В.М. Глушкова НАН України з компанією Motorola, і інсерційний підхід став основою системи VRS (Verification of Requirements Specifications) [4]. Ця система була призначена для автоматичної верифікації формальних вимог до проєктів програмного та апаратного забезпечення, для чого, відповідно, було розроблено технологію формалізації текстових та напівформальних вимог. Пізніше цю технологію було застосовано до верифікації дизайну систем та генерації тестових сценаріїв із заданим покриттям.

Після перших успішних впроваджень у телекомунікаційних проєктах компанії Motorola коло предметних галузей використання системи VRS значно розширилося: мережеві протоколи, мікропроцесорне середовище, автомобільна промисловість тощо. Останнім часом алгебраїчне моделювання впроваджується у сфері кібербезпеки, біології, економіки, права. Досвід таких інституцій, як Агентство передових оборонних дослідницьких проєктів США (DARPA), та провідних ІТ-компаній, наприклад Amazon, Google та Intel, свідчить, що формальні методи, зокрема алгебраїчний підхід, має бути покладено в основу всіх сучасних інструментів, які використовуються при проєктуванні, дослідженні та аналізі складних систем. Важливість застосування алгебраїчного підходу зумовлена також створенням сучасних ефективних програм, що виконують автоматичне доведення тверджень та розв'язок задач у різних теоріях.

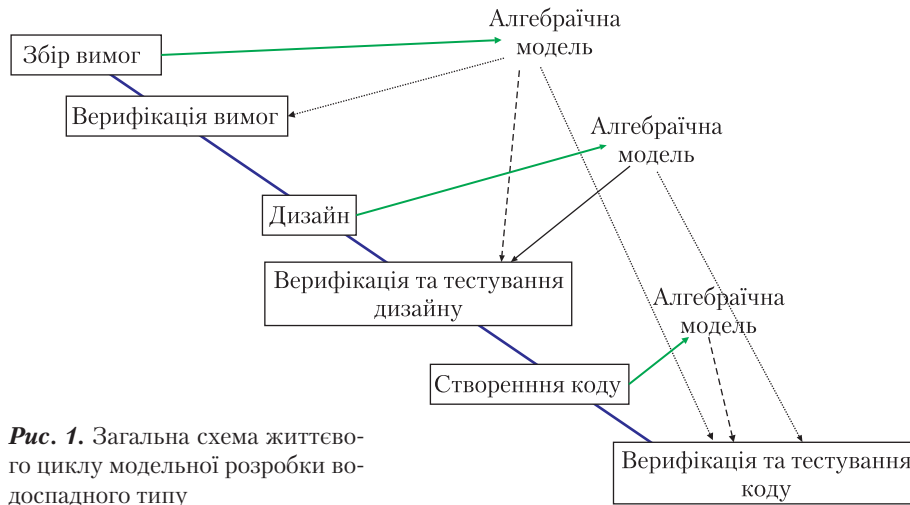
**Алгебра поведінок.** У 1997 р. британський учений Девід Гільберт (David R. Gilbert) та український кібернетик академік НАН України Олександр Адольфович Летичевський (1935–2019) розробили теоретичні основи інсерційного моделювання, зокрема алгебру поведінок [5]. Відмінністю інсерційного моделювання від попередніх теорій формальних

процесів було використання понять «агент» та «середовище». Сценарії поведінок агентів можуть породжуватися в багаторівневому середовищі, тобто сам агент може бути середовищем для інших агентів. Формально алгебра поведінок визначається як двохосновна алгебра над множинами поведінок та дій агентів. Вона містить операцію префіксингу та операцію недетермінованого вибору поведінок і включає три термінальні константи: успішне припинення  $\Delta$ , тупик  $0$  та невідома поведінка  $\perp$ . Крім того, алгебра поведінки розширена двома операціями: паралельні ( $\parallel$ ) та послідовні ( $;$ ) композиції поведінок. Терм, створений з операцій алгебри поведінки над поведінками та діями, формує вираз алгебри поведінок.

Семантика дій визначається перед- та післяумовою, що характеризують допустимість дій агента в середовищі та відповідну зміну середовища. Символьне моделювання поведінки агента визначається послідовністю його дій.

У різних предметних галузях агент може мати свій тип або набір атрибутів з відповідними простими типами. Формули перед- та післяумови є формулами над множиною атрибутів у відповідній теорії. При формалізації поведінки агентів у певній предметній галузі на різних рівнях абстракції використовують теорії булевої алгебри, цілочислової та ірраціональної арифметики, теорії перелічувальних символічних типів. Для створення середовищ моделей програм у мережевому та хмарному оточенні застосовують теорії, які містять операції та предикати над байтами і бітами.

**Розроблення систем високої надійності.** Найважливішою сферою використання алгебраїчного підходу є розроблення систем, критичних до безпеки. В Інституті кібернетики ім. В.М. Глушкова НАН України алгебраїчне моделювання впроваджено в модельний спосіб розроблення програмного та апаратного забезпечення. Модельний метод передбачає, що на кожному етапі розроблення, зокрема на стадіях усталення вимог, дизайну, кодування і тестування, з використанням формальних методів створюються відповідні моделі, призначені для верифікації та валідації системи.



**Рис. 1.** Загальна схема життєвого циклу модельної розробки водоспадного типу

Сучасні стандарти розроблення критичних до безпеки систем у медицині, авіакосмічній та автомобільній промисловості вже містять вимоги до використання відповідних формальних методів.

Ціна помилки, допущеної на ранніх стадіях розроблення критичних систем, може виявитися дуже високою. Недостатня надійність системи може вкрай негативно вплинути на загальний перебіг процесу реалізації проєкту, зокрема на його якість, собівартість та терміни виконання. Тому процедури формальної верифікації та тестування слід застосовувати як до системних вимог, так і до дизайну та програмного коду. Для цього на відповідних етапах розроблення системи створюють моделі формальних вимог, модель дизайну та модель коду. Ці моделі можуть бути отримані зі специфікацій формальних мов, таких як UML [6], SysML [7], BPMN [8], та мов програмування автоматичною трансляцією у специфікації алгебри поведінок. Маючи алгебраїчну модель, можна впровадити процедуру верифікації, використовуючи формальні методи, розроблені в рамках алгебри поведінок. Основними методами є символічне моделювання, методи алгебраїчного зіставлення та автоматичне доведення тверджень. Такі методи дають змогу верифікувати специфікації на недетермінізм, повноту, збереження властивостей безпеки та доведен-

ня життєздатності. Зазначені моделі є також джерелом тестів, як для специфікації дизайну, так і для програмного коду.

Загальну схему життєвого циклу модельної розробки водоспадного типу наведено на рис. 1.

Алгебраїчний та інсерційний підходи ефективні для розподілених мереж та систем, для яких у зв'язку з нескінченною або великою кількістю станів традиційні методи тестування та верифікації можуть не дати гарантованого покриття. Формальні методи завдяки тому, що вони дозволяють застосовувати абстракції різних рівнів, дають змогу вирішувати такі завдання для досить широкого класу моделей.

Модельний спосіб розроблення програмних систем було застосовано також для створення апаратного забезпечення. У рамках співробітництва Інституту кібернетики ім. В.М. Глушкова НАН України з Національним аерокосмічним університетом ім. М.Є. Жуковського «Харківський авіаційний інститут» та ТОВ «Науково-виробниче підприємство «Радікс» – виробником мікроелектроніки для потреб атомної енергетики України, було проведено апробацію модельного способу розроблення апаратних систем [9]. На кожному етапі V-модельного життєвого циклу системи для дизайну мікроелектроніки використовуються специфікації формальних мов, таких як

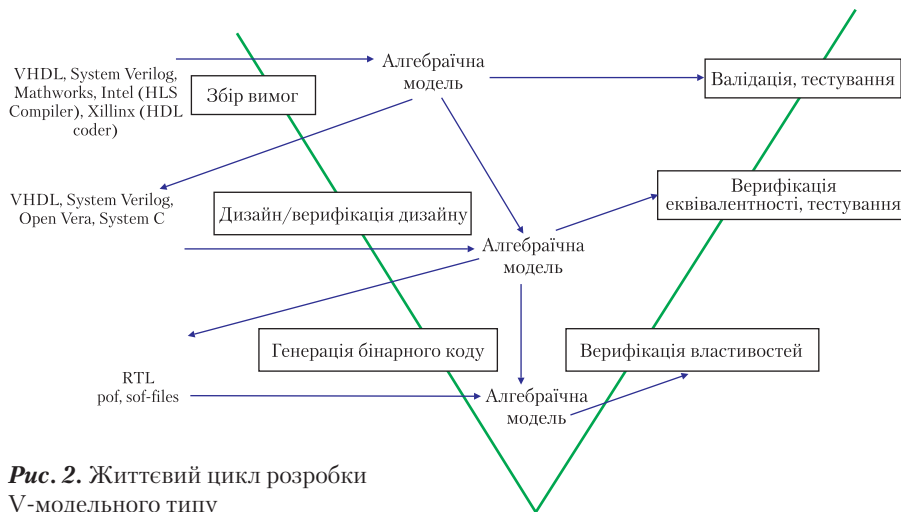


Рис. 2. Життєвий цикл розробки V-модельного типу

VHDL [10], System Verilog [11], та специфікації формальних вимог до апаратного забезпечення. Загальну схему такого циклу наведено на рис. 2.

**Завдання кібербезпеки.** Специфіка сучасних методів кібербезпеки полягає в постійній адаптації технології захисту до нових атак зловмисників. Нові методи проникнення та ураження програмних і апаратних систем з'являються щодня, тому традиційні технології антивірусних та інших засобів безпеки можуть виявитися неефективними. Алгебраїчний підхід дає змогу охоплювати класи шкідливих дій з використанням абстракцій різного рівня. Ефективність використання алгебраїчного підходу було доведено на міжнародному змаганні з кібербезпеки, проведеному корпорацією DARPA [12]. Перші три місця на ньому посіли компанії, які використовують символічне моделювання.

В Інституті кібернетики ім. В.М. Глушкова НАН України розроблено технологію алгебраїчної формалізації можливих вразливостей у бінарному коді програми. Поведінка програми при використанні зловмисником вразливості записується у вигляді виразів алгебри поведінок. Наприклад, вразливість «ураження програмного стеку» складається з трьох поведінкових виразів: точка входу в програму, створення нового стекового простору для запису

змінних процедури та запис до стеку з метою пошкодження даних або перехоплення управління зловмисником. У такий спосіб було формалізовано певну частину відомих вразливостей зі світових баз даних.

Розроблені алгоритми символічного моделювання та алгебраїчного зіставлення дозволяють ефективно знаходити вразливість за її алгебраїчним шаблоном на рівні бінарного коду [13], зокрема на рівні машинних інструкцій мови Intel x86. Ефективність алгебраїчного методу полягає в подоланні проблеми помилкових виявлень (false positive) та покритті більш широкого класу вразливостей. Відомо, що алгебраїчні методи підвищують обчислювальну складність, але бурхливий розвиток дедуктивних інструментів та програм-розв'язувачів [14] в останнє десятиліття дав можливість використовувати символічні обчислення в усіх сферах комп'ютерних технологій.

Алгебраїчний підхід до формалізації вразливостей, зокрема використання абстракцій, дає змогу знаходити прояви невідомих вразливостей, що можуть стати мішенню для шкідливих дій зловмисників. Ще один із методів пошуку так званих «вразливостей нульового дня» — це метод алгебраїчного фазингу (fuzzing), за допомогою якого за попереднім аналізом коду можна виявити критичні вхідні дані, що зламують програму.

Виявлення вразливостей у бінарному кодї є важливим етапом у забезпеченні захисту систем об'єктів критичної інфраструктури, насамперед при встановленні та експлуатації програмних систем. Придбані системи потенційно можуть містити вразливості, які уможливають неавторизоване проникнення або пошкодження даних. Принаймні такий етап перевірки на вразливості є необхідним при розробленні програмного забезпечення як на стадії кодування, так і при тестуванні програм.

Інше використання алгебраїчного підходу можливе при виявленні кібератак під час функціонування програмної системи. Алгебраїчний шаблон зламу або проникнення в систему можна описати відносно дій зловмисника. Аналізуючи трафік та дії в системі або мережі, алгоритм алгебраїчного зіставлення з шаблоном поведінки зловмисника просигналізує в разі її виявлення.

Для виявлення зловмисників у мережі або хмарному середовищі алгебраїчний підхід використовується також у комбінації з методами машинного навчання [15]. Модель класифікації, яка попередньо виявляє підозру на поведінку зловмисника на рівні нейронної мережі, може активувати алгебраїчні алгоритми для точного виявлення атаки.

Технологію формалізації вразливостей у термінах алгебри поведінок застосовують і для виявлення нештатних функціональностей, які можуть бути внесені в систему програмістом-розробником для подальшої експлуатації з метою проникнення або пошкодження системи. Методи виявлення таких «закладок» (backdoors) ґрунтуються на методах алгебраїчного моделювання та застосовуються як до програмних систем, так і для пристроїв мікроелектроніки та інших апаратних систем.

**Гібридні інтелектуальні системи.** Наукова спадщина академіка О.А. Летичевського охоплює низку важливих розробок та перспективних ідей, зокрема впровадження в інсерційне моделювання неперервних процесів [16].

Ця ідея та начерки теорії стосуються аналізу і верифікації процесів у гібридних інтелектуальних системах, що поєднують взаємодію

фізичних об'єктів та дискретних обчислювальних процесів. По суті для таких систем використовується комбінація алгебри поведінок та фізичних процесів, що описуються диференційними рівняннями і фігурують у дискретній системі як процес переходу між станами. Відмінність від сучасних гібридних систем, таких як автомат Хенцінгера [17], полягає в тому, що неперервні процеси розглядаються в контексті взаємодії агентів фізичних систем у багаторівневих середовищах. Завдяки такій синергії гібридний підхід збагачує можливості вивчення природних, зокрема біологічних, об'єктів.

Гібридний підхід було застосовано у спільних роботах Інституту кібернетики ім. В.М. Глушкова НАН України та Херсонського державного університету для формалізації хімічних і біологічних взаємодій. Можливість будувати абстракції на різних рівнях представлення моделей дозволила розглядати взаємодії агентів та середовищ від молекулярного рівня до рівнів вищих організацій матерії.

На рівні молекулярної взаємодії розглядаються середовища, в яких атоми і молекули є агентами, що змінюють свої стани та структури. Дії таких агентів, що формалізуються алгебраїчними рівняннями, моделюють переходи електронів на орбіталях, встановлення різновидів молекулярного зв'язку, розклад молекул на складові, утворення нових агентів та інші можливі взаємодії. У формальній моделі присутня також неперервна компонента, яка описує, наприклад, перебіг хімічної реакції.

У системі інсерційного моделювання проведено низку експериментів зі взаємодії молекул органічних речовин. Систему було інтегровано з відомими форматами представлення молекул, що дає можливість використовувати інформацію про речовини із всесвітніх банків даних, зокрема з банку білків.

Наразі планується продовжити експерименти з гібридними системами в хімії та біології. Алгебраїчне моделювання молекулярної взаємодії можна використовувати і для розгляду агентів та середовищ на іншому рівні абстракції. Зокрема, передбачається застосування цієї технології для вивчення взаємодії вірусу з

клітинами. Такі дослідження в системі інсерційного моделювання дадуть змогу вивчати поведінку та властивості агентів клітинного середовища, наприклад з метою розроблення вакцин в умовах еволюції вірусів.

**Технологія блокчейн.** Технологія блокчейн, яка основана на принципах децентралізації та алгоритмах консенсусу, сьогодні дедалі ширше впроваджується в різні сфери економічної та суспільної діяльності як технологія, що забезпечує захищеність від стороннього втручання, цілісність даних та справедливість вибору. Проте складність систем на блокчейн-платформах зумовлює можливість появи помилок, які не так просто виявити. З іншого боку, виникнення цієї нової технології і поширення використання криптовалют спричинили появу нових технік зламу та втручань у роботу систем.

При використанні алгебраїчного моделювання як агентів розглядають вузли мережі, в рамках якої функціонує протокол блокчейну. Агенти обмінюються транзакціями, формуючи блокчейн, але при цьому може з'явитися зловмисник, який використовуватиме вразливість протоколу з метою викрадення криптовалюти. Такі ситуації трапляються при функціонуванні «розумних контрактів» (smart contracts) [18] у рамках протоколів блокчейну. В цьому разі також можна формалізувати відомі поведінки зловмисника як алгебраїчні шаблони, що дає змогу перевіряти стійкість «розумного контракту» до атак та наявність у ньому вразливостей.

У різних галузях сучасної індустрії останнім часом з'явилося багато систем на основі блокчейн-платформ, зокрема фінансові, енергетичні та логістичні системи. В Інституті кібернетики ім. В.М. Глушкова НАН України розроблено технологію формалізації, верифікації та тестування таких платформ з використанням алгебраїчного моделювання [19]. Також розглядається можливість використання гібридного підходу, який поєднує алгебраїчний підхід та методи машинного навчання для формування моделі класифікації поведінки.

**Економіка та право.** У спільних з Херсонським державним університетом роботах ал-

гебраїчне моделювання та інсерційний підхід було застосовано для створення економічних та правових моделей.

В економічних системах як взаємодіючі агенти розглядаються різні об'єкти, що взаємодіють один з одним у рамках економічної діяльності, а саме — державні органи управління, підприємства, банки, групи населення. Завданням для використання алгебраїчного моделювання в економіці є вивчення властивостей економічної системи, наприклад економічної рівноваги. Властивості описують формулами в алгебрі поведінок і за допомогою символічного моделювання з'ясовують, чи досяжна ситуація, коли та чи інша властивість проявляється, або чи є серед множини сценаріїв такий, що приводить до порушення певної властивості системи. В економіці алгебраїчна модель з більшою точністю може передбачити розвиток подій, оскільки вона, на відміну від імітаційного моделювання, працює з множиною сценаріїв.

У проектах, що реалізуються на основі блокчейн-платформ, використовують добре формалізовані алгоритми із застосуванням токенів — умовних грошових одиниць. Дослідження властивостей таких систем та передбачення небажаних сценаріїв є важливим завданням, яке успішно вирішується за допомогою алгебраїчного підходу [20].

У моделюванні правових систем в рамках експерименту було формалізовано Податковий кодекс України у вигляді моделі взаємодії агентів — платників податків [21]. Одним із завдань, для вирішення якого може бути використано алгебраїчне моделювання, є перевірка правомірності дій платника податків відповідно до Податкового кодексу та виявлення порушень. Це може бути застосовано як під час моніторингу функціонування агентів, так і при розгляді судових рішень та суперечливих ситуацій.

Формальна модель законів дає також змогу перевірити їх на властивості повноти та взаємосуперечливості положень окремих статей. Одним із прикладів такого використання є доведення суперечливості в положеннях старої

версії Податкового кодексу на основі прецеденту «засуджений ПДВ» [22].

На сьогодні алгебраїчний підхід та методи символічних обчислень все ширше застосовуються в наукових дослідженнях та в процесі створення сучасних програмних систем. Нові ефективні інструменти, такі як дедуктивні системи, програми-розв'язувачі, засоби авто-

матичного доведення, є не лише предметом обговорення на наукових конференціях, вони вже використовуються в практичній діяльності багатьох передових індустріальних компаній. Тому подальший розвиток таких підходів, особливо в поєднанні з іншими методами штучного інтелекту, прогнозується як один з найважливіших напрямів у сучасній індустрії.

## REFERENCES

### [СПИСОК ЛІТЕРАТУРИ]

- Letichevsky A., Lyaletski A., Morokhovets M. Glushkov's evidence algorithm. *Cybernetics and Systems Analysis*. 2013. 49(4): 489–500. DOI: <https://doi.org/10.1007/s10559-013-9534-z>  
[Летичевський А.А., Лялецкий А.В., Мороховець М.К. Алгоритм очевидності Глушкова. *Кібернетика та системний аналіз*. 2013. Т. 49, № 4. С. 3–16.]
- Kapitonova J., Letichevsky A. Algebraic Programming in the APS System. In: *ISSAC '90: Proceedings of the international symposium on symbolic and algebraic computation* (20-25 August, 1990, Tokyo, Japan). P. 68–75. DOI: <https://doi.org/10.1145/96877.96896>
- Letichevsky A., Letychevskiy O., Peschanenko V. Insertion Modeling and Its Applications. *Computer Science Journal of Moldova*. 2016. 24(3): 357–370. <http://www.apsystems.org.ua/uploads/doc/aps/APSv3.eng.pdf>
- Letichevsky A., Kolchin A., Letychevskiy O., Potiyenko S., Volkov V., Weigert T. Formal Requirements Capturing using VRS system. In: Voronkov A., Kovács L., Bjorner N. (eds). *WING 2010. Workshop on Invariant Generation 2010* (21 July, 2010, Edinburgh, UK). Vol. 1. P. 148–149. DOI: <https://doi.org/10.29007/q6mc>
- Letichevsky A., Gilbert D. A Model for Interaction of Agents and Environments. In: Bert D., Choppy C., Mosses P.D. (eds). *Recent Trends in Algebraic Development Techniques. WADT 1999. Lecture Notes in Computer Science*. Vol. 1827. Berlin, Heidelberg: Springer, 2000. P. 311–328. DOI: [https://doi.org/10.1007/978-3-540-44616-3\\_18](https://doi.org/10.1007/978-3-540-44616-3_18)
- Booch G., Rumbaugh J., Jacobson I. *Unified modeling language user guide*. Addison-Wesley, 2005.
- Burger E. *Flexible views for view-based model-driven development*. KIT Scientific Publishing, 2014.
- Silver B. *BPMN method and style*. Cody–Cassidy Press, 2011.
- Letychevskiy O., Odaruschenko O., Peschanenko V., Kharchenko V., Volkov V. Modeling Method for Development of Digital System Algorithms Based on Programmable Logic Devices. *Cybernetics and Systems Analysis*. 2020. 56: 710–717. DOI: <https://doi.org/10.1007/s10559-020-00289-8>  
[Летичевський О., Одарущенко О., Песчаненко В., Харченко В., Волков В. Модельний спосіб розроблення алгоритмів цифрових систем на програмованих логічних інтегральних схемах. *Кібернетика та системний аналіз*. 2020. Т. 56, № 5. С. 29–37.]
- Coelho D. *The VHDL handbook*. Springer Science & Business Media, 1989.
- Sutherland S., Davidmann S., Flake P. *System Verilog for Design*. Springer Science & Business Media, 2006.
- Fraze D. Cyber Grand Challenge (CGC) (Archived). DARPA. <https://www.darpa.mil/program/cyber-grand-challenge>
- Letychevskiy O. Two-Level Algebraic Method for Detection of Vulnerabilities in Binary Code. In: *Proc. of 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems* (18-21 September, 2019, Metz, France). DOI: <https://doi.org/10.1109/IDAACS.2019.8924255>
- Robere R., Kolokolova A., Ganesh V. The Proof Complexity of SMT Solvers. In: Chockler H., Weissenbacher G. (eds). *Computer Aided Verification. CAV 2018. Lecture Notes in Computer Science*. Vol. 10982. Springer, Cham, 2018. DOI: [https://doi.org/10.1007/978-3-319-96142-2\\_18](https://doi.org/10.1007/978-3-319-96142-2_18)
- Letychevskiy O., Polhul T. Detection of Fraudulent Behavior Using the Combined Algebraic and Machine Learning Approach. In: *Proc. of IEEE International Conference on Big Data* (9-12 December, 2019, Los Angeles, USA). DOI: <https://doi.org/10.1109/BigData47090.2019.9006546>
- Letichevsky A. Algebraic Interaction Theory and Cyber-Physical Systems. *Journal of Automation and Information Sciences*. 2017. 49(9): 1–19. DOI: <https://doi.org/10.1615/JAutomatInfScien.v49.i9.10>

- [Летичевский А.А. Алгебраическая теория взаимодействия и кибер-физические системы. *Проблемы управления и информатики*. 2017. № 5. С. 37–55.]
17. Henzinger T.A. The theory of hybrid automata. In: Inan M.K., Kurshan R.P. (eds). *Verification of Digital and Hybrid Systems*. NATO ASI Series (Series F: Computer and Systems Sciences). Vol. 170. Springer, Berlin, Heidelberg. DOI: [https://doi.org/10.1007/978-3-642-59615-5\\_13](https://doi.org/10.1007/978-3-642-59615-5_13)
  18. Alharby M., Moorsel A. Blockchain Based Smart Contracts. A Systematic Mapping Study. In: *Proc. of International Conference on Cloud Computing, Big Data and Blockchain* (15-17 November, 2018, Fuzhou, China). DOI: <https://doi.org/10.5121/csit.2017.71011>
  19. Letychevskiy O., Peschanenko V., Radchenko V., Orlovskiy M., Sobol A. Algebraic approach to verification and testing of distributed applications. In: *Proc. of Blockchain and Internet of Things Conference* (7-9 July, 2019, Okinawa, Japan). DOI: <https://doi.org/10.1145/3343147.3343159>
  20. Letychevskiy O., Peschanenko V., Radchenko V., Poltoratzkyi M., Mogylyko S., Kovalenko P. Formal Verification of Token Economy Models. In: *Proc. of International Conference on Blockchain and Cryptocurrency* (14-17 May, 2019, Seoul, South Korea). DOI: <https://doi.org/10.1109/BLOC.2019.8751318>
  21. Letychevsky A., Letychevskiy O., Peschanenko V., Poltoratzky M. An Algebraic Approach for Analyzing of Legal Requirements. In: *Proc. of International Requirements Engineering Conference Workshops (REW)*. (4-8 September, 2017, Lisbon). DOI: <https://doi.org/10.1109/REW.2017.51>
  22. «Zasudzhenyi» PDV abo Pretsedent na koryst platnyka podatku. *Konsultant bukhhaltera*. No. 16 (400). 16.04.2007. [http://cons.parus.ua/\\_d.asp?r=03WMGd7e3c4816c93692e4d5ba8e0b8234dec](http://cons.parus.ua/_d.asp?r=03WMGd7e3c4816c93692e4d5ba8e0b8234dec)  
[«Засуджений» ПДВ або Прецедент на користь платника податку. *Консультант бухгалтеря*. № 16 (400). 16.04.2007.]

*Oleksandr O. Letychevskiy*

ORCID: <https://orcid.org/0000-0003-0856-9771>

Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine, Kyiv, Ukraine

#### ALGEBRAIC MODELING AND ITS APPLICATION

The article is devoted to the scientific development of the Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine on the application of algebraic and insertional modeling technologies created on the basis of behavioral algebra. Technologies of formalization, algebraic verification, and testing of software and hardware specifications within the model-driven development method are considered. The use of algebraic modeling in biological research, development of systems based on blockchain platforms, analysis of legal and economic models is covered. One of the main areas of application of these technologies is the field of cybersecurity, which uses the method of algebraic matching and formalization of patterns of vulnerabilities and cyberattacks.

**Keywords:** algebraic modeling, code vulnerabilities, model-driven development, insertion modeling, formal verification, model-based testing, hybrid intelligent systems.