Методологія побудови багатоконтурних систем безпеки

Сергій Євсеєв
доктор технічних наук, професор, завідувач кафедри кібербезпеки,
НТУ «Харківський політехнічний інститут» МОН України, м. Харків,
Україна, ORCID: https://orcid.org/0000-0003-1647-6444,
e-mail: Serhii.Yevseiev@gmail.com

Олена Ахієзер
кандидатка технічних наук, професорка, завідувачка кафедри
комп'ютерної математики та аналізу даних,
НТУ «Харківський політехнічний інститут» МОН України, м. Харків,
Україна, ORCID: https://orcid.org/0000-0002-7087-9749,
e-mail: Olena.Akhiiezer@khpi.edu.ua

Запропоновано методологію побудови багатоконтурних систем безпеки об'єктів критичної інфраструктури, яка ґрунтується на принципово новому підході до побудови таких систем. В основу методології покладено принцип синергізму.
Ключові слова: *об'єкти критичної інфраструктури; багатоконтурні системи захисту інформації; постквантові алгоритми.*

Methodology for Creating Multi-Circuit Security Systems

Serhii Yevseiev, Olena Ahiiezer

The methodology for creating multi-circuit security systems for critical infrastructure facilities has been proposed, which is based on a fundamentally new approach to the construction of such systems. The methodology stems from the principle of synergy.
Keywords: *critical infrastructure facilities; multicircuit information security systems; post-quantum algorithms.*

В умовах збройної агресії російської федерації проти України, яка досі триває, безпека людини, суспільства й держави суттєво залежать від надійного функціювання об'єктів критичної інфраструктури. Окрім фізичних впливів на такі об'єкти летальною зброєю, російська федерація не полишає спроб разом зі своїми сателітами впливати іншими засобами — кібератаками на системи управління об'єктів критичної інфраструктури через кіберпростір та з кіберпростору. Ураховуючи транскордонність кіберпростору та високий рівень інформатизації об'єктів критичної інфраструктури як в Україні, так і у світі, наприклад, об'єктів ядерної енергетики (Запорізька та Чорнобильська атомні станції), об'єктів водопостачання (Каховська

та Київська ГЕС), систем управління військами та зброєю (Єдина автоматизована система управління (ЄАСУ) Збройними силами України та її складових) тощо, ризики збільшуються й становлять глобальну загрозу для людства. Ситуація ускладнюється тим, що об'єкти критичної інфраструктури, які функціюють у єдиному інформаційному просторі й підтримують широкий спектр сучасних інформаційних технологій, і надалі залишаються вразливими до загроз нового типу.

Запропонована методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури ґрунтується на принципово новому підході до побудови таких систем. Підґрунтям методології є принцип синергізму. Інтелектуалізація моделей та синергетичні ефекти, що виникають за їх синтезу, дають змогу отримувати нові емерджентні властивості систем управління та безпеки об'єктів критичної інфраструктури. Зокрема, на основі одержаних моделей відкрито ефект побудови N-контурних інтелектуальних систем управління та безпеки з наперед заданими показниками стійкості до загроз визначеного (квантового) або прогнозованого (постквантового) типу залежно від приналежності об'єктів критичної інфраструктури. Розроблена методологія призначена для запобігання проявам несанкціонованого втручання в штатні режими функціювання об'єктів критичної інфраструктури та застосовується для прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури внаслідок застосування кіберзброї недружніми до України державами або терористичними кіберугрупованнями. На основі розробленої методології синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури, принципово різних за своїми властивостями, забезпечується безперервність виконання основних функцій інтелектуальними системами управління об'єктів критичної інфраструктури за одночасного гарантованого (заданого) рівня захищеності таких систем, що має критично важливе значення для подальшого розвитку галузі інформаційної безпеки держави в інтересах підвищення рівня національної безпеки України, забезпечення безпеки громадян, захисту їх прав та свобод.

Запропонована методологія багатоконтурних систем безпеки об'єктів критичної інфраструктури надає об'єктивну оцінку будь-якої інфраструктури об'єктів критичної інфраструктури (будь-якої галузі), що забезпечує її універсальність (рис. 1). Виявлена залежність рівня захищеності контуру бізнес-процесів системи безпеки, яка визначається часткою успішно проведених атак відносно їх загальної кількості, від часу перемикання із захисту одного вектора безпеки до іншого, що забезпечує за збільшення інтервалу на перемикання з одного вектору загроз на інший удвічі, кількість успішних атак зменшення в 1,76 рази. Під час побудови багатоконтурних систем захисту враховують фізичні складові інфраструктури та формують зовнішній та внутрішній контури безпеки.

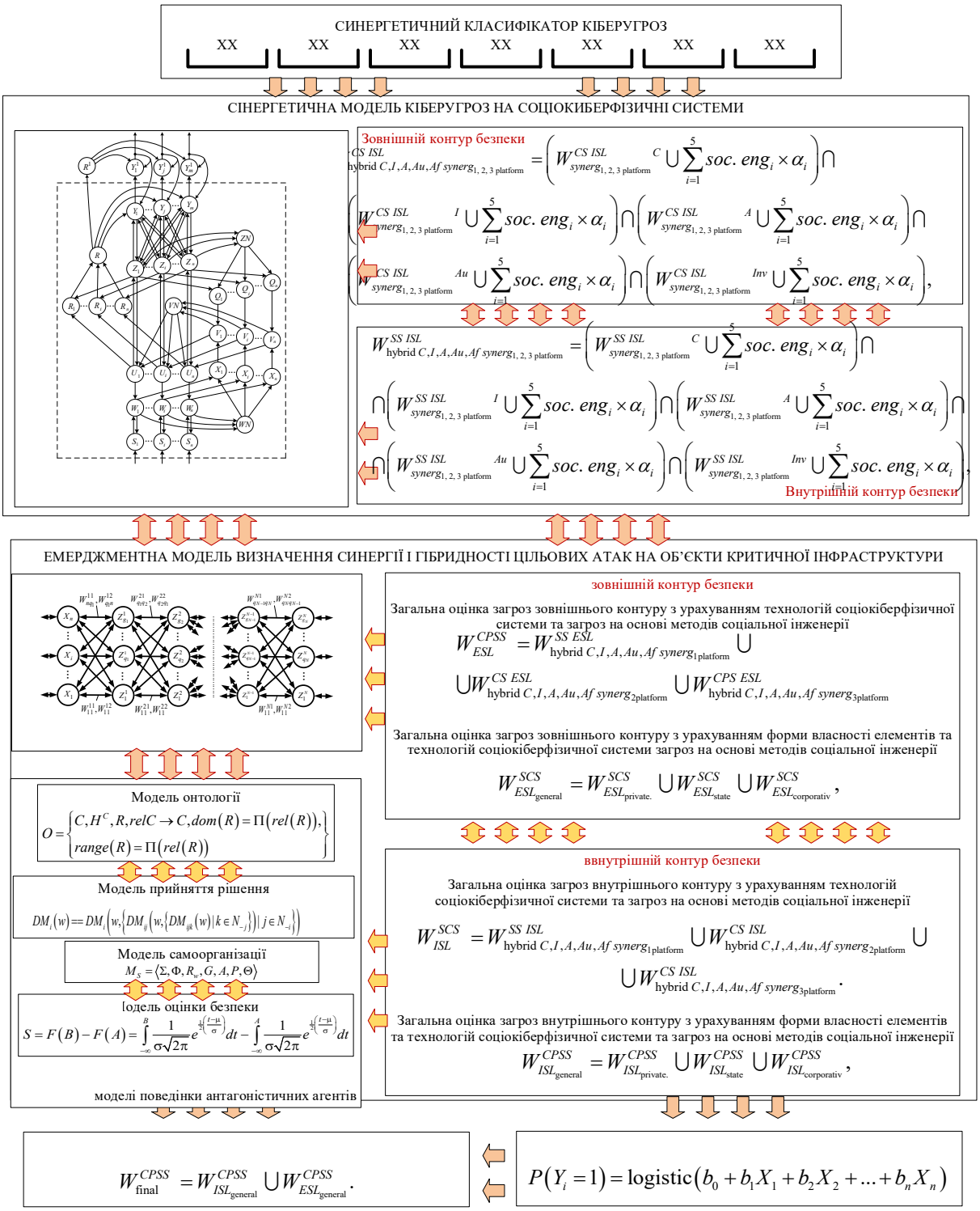

Рис. 1. Схема методології побудови багатоконтурних систем безпеки

Запропоновані механізми безпеки ґрунтуються на постквантових алгоритмах, які формують несиметричні криптосистеми — крипто-кодові конструкції Мак-Еліса та Нідеррайтера на основі алгеброгеометричних (еліптичних, модифікованих еліптичних кодах, збиткових кодах та LDPC-кодах), що дає змогу будувати криптосистеми з різним показником стійкості й у такий спосіб забезпечити застосування в будь-якої системі

безпеки об'єктів критичної інфраструктури. Основною відмінністю від відомих підходів є збереження рівня пропускних можливостей бездротового каналу інтегровано забезпечити необхідний рівень захищеності (криптостійкості) каналу (криптостійкість на основі постквантових алгоритмів на рівні 10^{25}–10^{35} групових операцій), достовірності ($P_{пом}$ не нижче 10^{-9}–10^{-12}). Застосування запропонованого синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури забезпечує застосування стандартних протоколів та необхідний рівень стійкості в умовах появи повномасштабного квантового комп'ютера. Розроблені алгоритми моделювання трафіка інтегральних потоків даних інфокомунікаційних мереж об'єктів критичної інфраструктури дають змогу поліпшити адекватність моделей реальному трафіку порівняно зі стандартними алгоритмами моделювання, до того ж сумарне відхилення змодельованого трафіка від реального зменшилося до 15%.

Перелік джерел посилання

1. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури : монографія / С. П. Євсеєв, О. Ю. Заковоротний, О. В. Мілов, Г. А. Кучук, О. А. Галуза, М. В. Коваль, О. В. Войтко, Р. В. Грищук. Харків, 2024. 300 с. URL: https://www.kdpu-nt.gov.ua/uk/content/metodologiya-syntezu-modeley-intelektualnyh-system-upravlinnya-ta-bezpeky-obyektiv (дата звернення: 19.10.2024).
2. Synergy of building cybersecurity systems : monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov et al. Kharkiv, 2021. 188 p. DOI: 10.15587/978-617-7319-31-2 (дата звернення: 19.10.2024).
3. Моделювання систем безпеки об'єктів критичної інфраструктури : монографія / С. Євсеєв, Р. Грищук, К. Молодецька та ін. Харків, 2022. 196 с. DOI: 10.15587/978-617-7319-57-2 (дата звернення: 19.10.2024).
4. Моделі безпеки соціокіберфізичних систем : монографія/ С. Євсеєв, Ю. Хохлачова, С. Остапов та ін. Харків, 2023. 168 с. DOI: https://doi.org/10.15587/978-617-7319-72-5 (дата звернення: 19.10.2024).
5. Розробка моделі поведінки агентів-антагоністів в умовах кіберконфлікту / О. Мілов, С. Євсеєв, Є. Іванчеко та ін. *Східно-Європейський журнал підприємницьких технологій.* 2019. Т. 4. № 9(100) С. 6—19. DOI: 10.15587/1729-4061.2019.175978 (дата звернення: 19.10.2024).
6. Розробка сценарного моделювання інструментів конфлікту в системі безпеки на основі формальних граматик / О. Мілов, С. Євсеєв, А. Власов та ін. *Східно-Європейський журнал підприємницьких технологій.* 2019. Т. 6. № 9(102). С. 22—39. DOI: https://doi.org/10.15587/1729-4061.2019.184274 (дата звернення: 19.10.2024).

7. Моделювання конкурентної взаємодії «хижак-жертва» на прикладі двох інноваційних процесів / А. Воронін, О. Ахієзер, О. Галуза та ін. : *мат-ли XIII міжнар. конф. з передових комп'ют. інформ. технол. (ACIT)*. (Дігендорф, Німеччина, 21—23.09.2023). Дігендорф, 2023. DOI: 10.1109/ACIT58437.2023.10275538 (дата звернення: 19.10.2024).
8. Безпекова синергетика: кібернетичний та інформаційний аспекти : монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька / за заг. ред. докт. техн. наук, проф. Р. В. Грищука. Житомир, 2019. 280 с. URL: https://www.researchgate.net/publication/332762487_Bezpekova_sinergetika_kiberneticnij_ta_informacijnij_aspekti_monografia (дата звернення: 19.10.2024).
9. Грищук Р. В. Методологія побудови багатокритерійних диференціально-ігрових моделей та методів. *Технологічний аудит та резерви виробництва*. 2013. № 5 (13). С. 43—45. URL: http://nbuv.gov.ua/UJRN/Tatrv_2013_5-5_20 (дата звернення: 19.10.2024).
10. В. Д. Дмитрієнко, О. Ю. Заковоротний. Архітектури та алгоритми функціонування нейронних мереж Хеммінга та Хебба, здатних донавчатися та розпізнавати нову інформацію. *Радіоелектроніка, інформатика, управління.* 2014. № 2. С. 100—109.
11. Кучук Г. А., Левашенко В. Г., Ляшенко О. С. Побудова системи підтримки прийняття рішень на основі нечітких даних. *Сучасні інформаційні системи*. 2020. Т. 4. № 4. С. 4—56. DOI: 10.20998/2522-9052.2020.4.07 (дата звернення: 19.10.2024).