Методологія побудови багатоконтурної системи безпеки у соціокіберфізичних системах

УДК 004.056. 5/.6/.7

Станіслав Мілевський[1], Сергій Євсеєв[2], Ірина Аксьонова[3]

Національний технічний університет «Харківський політехнічний інститут», [1]milevskiysv@gmail.com, [2]Serhii.Yevseiev@gmail.com, [3] ivaksyonova@gmail.com

Революційні зміни інфокомунікаційних та комп'ютерних мереж дозволили сформувати об'єднання в єдиний інформаційно-кібернетичний простір, систем на основі смарт-технологій, та зумовили формування соціокіберфізичних систем та перегляд об'єктів критичної інфраструктури. Як наслідок, суттєво зріс і спектр загроз для національної безпеки держави загалом. Ключовою і найбільш потенційно небезпечною є загроза зриву чи взяття під віддалений контроль процесів управління в соціокіберфізичних системах. При цьому під соціокіберфізичною системою розуміється еволюційне комплексування смарт-технологій із соціальними мережами месенджерами.

Наслідки у разі відсутності чи недосконалості механізмів забезпечення безпеки у соціокіберфізичній системі можуть мати колосальний та незворотний характер,. Вирішення всього комплексу питань, пов'язаних із забезпеченням кібербезпеки, інформаційної безпеки та безпеки інформації у соціокіберфізичній системі має вирішуватися в комплексі та нерозривно одне від одного. Просте комплексування сил і засобів у кожному окремому випадку задля забезпечення безпеки соціокіберфізичних системах (об'єктах критичної інфраструктури) є недоцільним, як із практичної, так і наукової точок зору. Відсутність інших альтернативних підходів спонукає нагальну необхідність у вирішенні проблеми, що склалася – підвищення захищеності інформації в соціокіберфізичних системах на основі нових невідомих до сьогодні підходів. Такий підхід потребує переформатування механізмів побудови систем захищеності елементів інфраструктури та потребує врахування побудови багатоконтурних систем захисту інформації на основі постквантових алгоритмів [1–5].

На рис. 1 представлено структурну схему методології побудови багатоконтурної системи захисту інформації. Основною відмінністю від відомих підходів є можливість синтезу як експертного, так і системного аналізу цільових загроз на соціокіберфізичні системи, а й можливість об'єктивної оцінки поточного стану захищеності інформації. Такий підхід дозволяє своєчасно реагувати на можливі зміни (модифікації) цільових загроз, а також враховувати їхню синергію та гібридність, можливість комплексування з методами соціальної інженерії. Пропоновані практичні рішення щодо забезпечення послуг безпеки на основі постквантових алгоритмів дозволяють забезпечити необхідний рівень стійкості конфіденційної інформації з різними рівнями їх секретності.

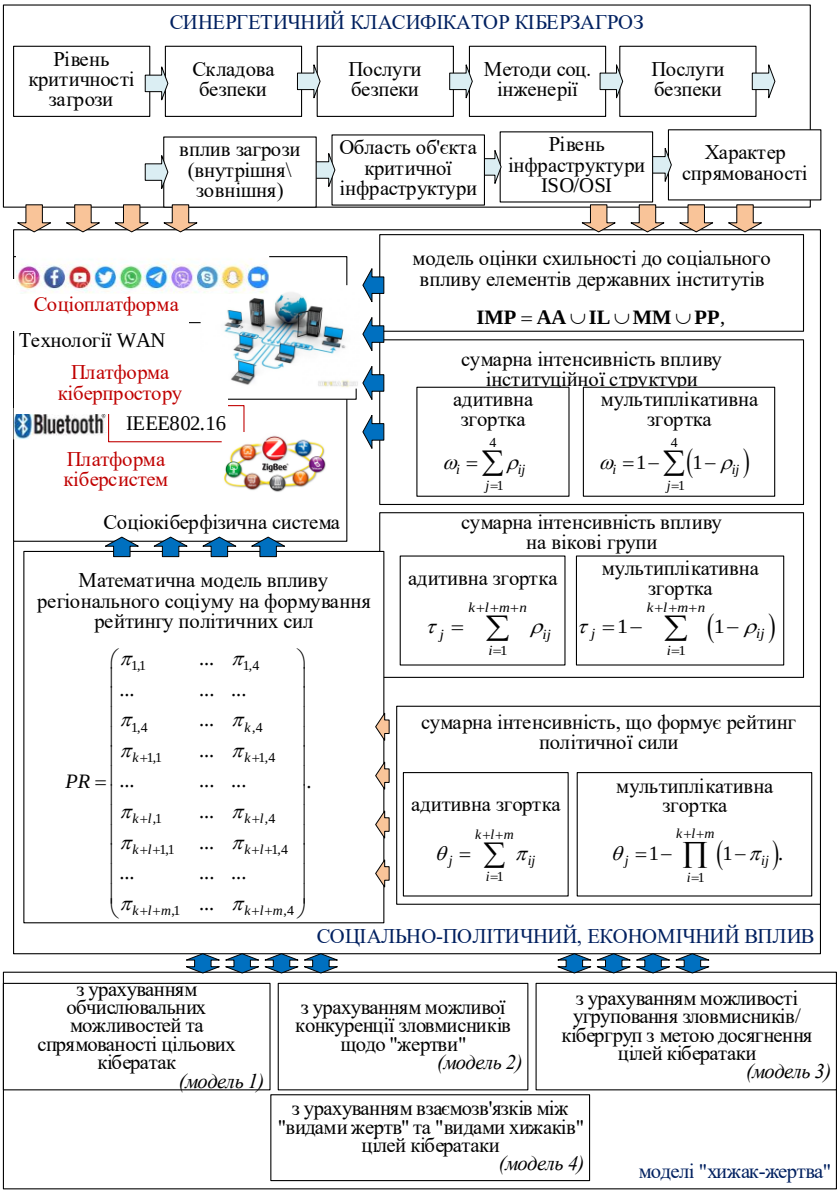

Рис.1. Структурна схема побудови системи оцінки поточного стану багатоконтурної системи захисту

Аналіз використання різних перешкодостійких кодів у крипто-кодових конструкціях та аналіз технологій побудови соціокіберфізичних систем на основі смарт-технологій показав, що використання різних кодів дозволяє диференціювати основні показники криптосистем та враховувати рівень таємності інформаційних ресурсів. Такий підхід дозволить знизити не тільки обчислювальні та ємнісні витрати, але й підвищити рівень безпеки за рахунок різних модифікацій та вибору завадостійких кодів. Даний механізм знизить можливість зламування крипто-кодових конструкцій та забезпечити необхідний рівень безпеки. Подано методологію побудови багатоконтурних систем захисту інформації, яка забезпечує об'єктивність оцінки поточного стану захищеності елементів інфраструктури соціокіберфізичних систем. Побудова багатоконтурної системи захисту на основі постквантових алгоритмів дозволить забезпечити необхідний рівень безпеки з урахуванням кількості секретності інформаційних ресурсів, їхньої циркуляції та зберігання.

1. Serhii Yevseiev, Oleksandr Milov, Nataliia Dzheniuk, Maksym Tolkachov, Tetiana Voitko, Mykhailo Prygara, Natalia Voropay, Oleksandr Shpak, Andrii Volkov, Oleksandr Lezik. Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies. 2023. 5/9 (125). P. 53–74
2. Nataliia Dzheniuk, Serhii Yevseiev, Bogdan Lazurenko, Oleksandr Serkov, Oleg Kasilov. Methods of information systems protection. Advanced Information Systems. 2023. Vol. 7, No. 4, P.80-85
3. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
4. Khoroshko V.O., Pavlov I.M., Bobalo Y.Ya., Dudykevich V.B. and others. Design of complex information protection systems. – Lviv: Ed. Lviv Polytechnic, 2020. – 320 pp.
5. Olexander Shmatko, Serhii Herasymov, Yurii Lysetskyi, Serhii Yevseiev, Oleksandr Sievierinov, Tetiana Voitko, Andrii Zakharzhevskyi, Alexander Nesterov, Kyrylo Bondarenko. Development of the synthesis method of the automated acceptance system in the management of information security channels. Eastern-European Journal of Enterprise Technologies. 2023. 6/9 (126). P. 39–49.