ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

https://doi.org/10.31649/1997-9266-2023-171-6-30-38

УДК 004. 942

М. М. Биков[1]
Т. В. Грищук[1]
О. О. Ковалюк[1]
В. В. Ковтун[1]
М. С. Юхимчук[1]

МОДЕЛЬ ЕКСПЛУАТАЦІЇ КІБЕРФІЗИЧНОЇ СИСТЕМИ В УМОВАХ ВПЛИВУ НЕГАТИВНИХ ЗОВНІШНІХ ФАКТОРІВ

[1]Вінницький національний технічний університет

Запропоновано математичний апарат для моделювання процесу експлуатації кіберфізичної системи в умовах впливу негативних зовнішніх факторів, який враховується відповідним параметром. На відміну від аналогів, модель досліджуваного процесу формалізується у параметричному просторі індикаторів безвідмовності, функційної безпечності та низки економічних показників. Узагальнювальним параметром в запропонованому математичному апараті є коефіцієнт ефективності, в якому враховуються накопичуваний параметр ефективності експлуатації кіберфізичної системи, супутній ризик від її експлуатації та обсяг ресурсів, закладених у заходи кібербезпеки на етапі проектування цільової системи. Аналітично описано зв'язок цього коефіцієнта з імовірністю переходу кіберфізичної системи в нефункціональний стан внаслідок реалізації негативного впливу попри супротив засобів кібербезпеки. Математичний апарат розвинуто в напрямку врахування похибок першого та другого роду у разі ідентифікації негативного впливу засобами кібербезпеки. Окремо досліджено випадок реакції засобів кібербезпеки на імітацію негативного впливу. Формалізовано пошук екстремального значення коефіцієнта ефективності від обсягу вкладених в заходи кібербезпеки ресурсів з урахуванням характеристичних параметрів простору, в якому цільова кіберфізична система експлуатується. Дослідження реальної кіберфізичної системи Ситуаційного центру департаменту кіберфізичних технологій Вінницької міської ради довело адекватність запропонованого математичного апарату.

Ключові слова: кіберфізична система, негативний фактор, процес експлуатації, математична модель, відмовостійкість, функційна безпека, ефективність.

Вступ

На сайті відомої аналітичної компанії Canalys подані результати дослідження, згідно з якими світовий ринок кібербезпеки в 2022 році збільшиться на 6…10 % і становитиме $57…60 млрд відповідно. Фахівці компанії сегментували ринок кібербезпеки на такі кластери як: безпека кінцевих точок, безпека мереж, безпека кіберфізичних систем, безпека кіберфізичних ресурсів, пошук і аналіз вразливостей. Згідно з прогнозом, найстрімкіше зростання очікує кластер безпеки кіберфізичних систем (12,5 %) і кластер пошуку та аналізу вразливостей (11 %). Наведена інформація є найкращим доведенням актуальності дослідження, результати якого викладені в цій статті, адже вони безпосередньо відносяться до першого з вищезгаданих кластерів і опосередковано — до другого.

Огляд аналогів

Найактуальнішою проблемою в сфері кібербезпеки є ідентифікація і опис негативних впливів або кіберзагроз. Саме достовірний результат їхньої ідентифікації є підставою для раціонального вибору засобів та методів знешкодження. Згадаємо лише загальновизнані методології, які застосо-

вуються для оцінки стану кібербезпеки, моделювання засобів захисту кіберфізичних ресурсів та ідентифікації негативних впливів на кіберфізичні системи. Йдеться про [1]—[5]: теорію ігор, нечіткі множини, теорію графів, мережі Петрі, теорію цифрових автоматів, теорію випадкових процесів тощо. Такий різновид випадкових процесів як марковські процеси знайшов широке застосування в моделюванні безвідмовності та інших атрибутів гарантоздатності технічних та кіберфізичних систем [6]—[8]. Викладені в статтях [9], [10] результати довели, що марковські процеси можна застосовувати для моделювання негативних впливів на кіберфізичні системи, якщо перші можна вважати стохастичними і незалежними. Виходячи з цих постулатів, застосування марківських процесів для моделювання процесу експлуатації кіберфізичних систем є допустимим.

Об'єктом дослідження є процес експлуатації кіберфізичної системи в умовах агресивного кіберпростору.

Предметом дослідження є марковська модель експлуатації кіберфізичної системи в умовах впливу типізованих негативних зовнішніх факторів.

Метою дослідження є аналітична формалізація цього процесу в параметричному просторі індикаторів безвідмовності, функційної безпечності та економічної ефективності з урахуванням потенційного впливу негативних факторів.

Моделі і методи

1. Постановка задачі дослідження

Нехай досліджувана кіберфізична система (ДКФС) в процесі експлуатації взаємодіє з агресивним зовнішнім кіберфізичним простором. Агресивність кіберпростору проявляється у неперіодичному негативному впливі зовнішніх факторів техногенного або суспільного походження. Реалізація такого негативного впливу на ДКФС оцінюється стохастичною величиною q і може спричинити перехід останньої в нефункціональний стан S_{off}. Імовірність такої події характеризується стохастичним параметром π, а втрати, які зазнає ДКФС в разі передчасного переривання процесу експлуатації, визначаються параметром d_0. Рівень безвідмовності ДКФС характеризуватимемо інтенсивністю збоїв $\lambda(t)$, а інтенсивність та ефективність з якою вона реалізує своє функціональне призначення позначатимемо параметрами $\mu(t)$ і w_0 відповідно. Параметр w_0 характеризує накопичуваний прибуток, який забезпечує функціонуюча ДКФС з моменту ініціації процесу експлуатації. Спроможність ДКФС протидіяти впливу негативних факторів закладається на етапі її проектування і характеризується обсягом закладених ресурсів *C*. Відповідно ефективність кіберімунної реакції ДКФС на імовірні негативні впливи можна описати функцією $\pi(C)$. З урахуванням введеного базису сформульовано *задачі дослідження*:

1. Формалізувати орієнтовану на практичне застосування модель процесу експлуатації ДКФС в агресивному кіберфізичному просторі;

2. Довести адекватність запропонованої моделі та апробувати її для описання процесу експлуатації реальної кіберфізичної системи.

2. Математична модель досліджуваного процесу

Перевизначимо для довільного моменту часу $t > 0$ характеристичні параметри ефективності і втрат з урахуванням детермінованих коефіцієнтів інфляції *r* та дисконтування *i*

$$d(t) = d_0 \gamma^t, \tag{1}$$

де $\gamma = (1+r)/(1+i)$, а $t = 0$ — момент початку експлуатації ДКФС.

Охарактеризуємо параметром $p_0(t)$ імовірність того, що в момент часу $t > 0$ ДКФС перебуває в функціональному стані S_{on}. Представимо цей стохастичний параметр в динаміці рівнянням

$$dp_0(t)/dt = -p_0(t) \cdot (q\pi\mu(t) + \lambda(t)). \tag{2}$$

За аналогією з (2), подамо в динаміці накопичуваний параметр ефективності експлуатації ДКФС $W(t)$

$$dW(t)/dt = -p_0(t)\cdot(1-q\pi)w(t) \tag{3}$$

та супутній ризик від її експлуатації $R(t)$

$$dR(t)/dt = p_0(t)\cdot q\pi\mu(t)d(t). \tag{4}$$

Співвідношення показників (3), (4) раціонально характеризує процес експлуатації ДКФС в умовах агресивного кіберпростору, якщо додатково врахувати закладений на етапі її проектування кіберімунний потенціал C $\beta(t)=W(t)/(R(t)+C)$. Якщо постулювати незалежність параметрів $\mu(t)$ і $\lambda(t)$, то розв'язок рівняння (2) в аналітичній формі визначимо як

$$p_0(t) = \exp(-t(q\pi\mu+\lambda)). \tag{5}$$

Виразимо в аналітичній формі розв'язки виразів (3) і (4) з урахуванням залежності (1)

$$W(t) = \frac{\mu w_0(1-q\pi)}{\ln\gamma-(q\pi\mu+\lambda)}\left(\exp\left(t\left(\ln\gamma-(q\pi\mu+\lambda)\right)\right)-1\right); \tag{6}$$

$$R(t) = \frac{q\pi\mu d_0}{\ln\gamma-(q\pi\mu+\lambda)}\left(\exp\left(t\left(\ln\gamma-(q\pi\mu+\lambda)\right)\right)-1\right). \tag{7}$$

Математичний аналіз виразів (6) і (7) дозволяє стверджувати, що за виконання умови

$$\ln\gamma-(q\pi\mu+\lambda)<0 \tag{8}$$

граничні значення параметрів *W* і *R* визначаються відповідними виразами

$$W_{\lim} = \frac{\mu w_0(1-q\pi)}{(q\pi\mu+\lambda)-\ln\gamma};\ R_{\lim} = \frac{\mu d_0 q\pi}{(q\pi\mu+\lambda)-\ln\gamma}.$$

За виконання умови (8) значення коефіцієнта $\beta(t)$ зростатиме, але загалом не перевищить граничного значення

$$\beta^{-}_{\lim} = \frac{w_0(1-q\pi)}{C(q\pi\mu+\lambda)/\mu+q\pi d_0}. \tag{9}$$

Якщо ж умова (8) не виконується, то значення коефіцієнта $\beta(t)$ все одно зростатиме, але загалом не перевищить граничного значення

$$\beta^{+}_{\lim} = \frac{w_0(1-q\pi)}{q\pi d_0}. \tag{10}$$

До слова, умова (8) може не виконуватись лише, коли рівень дисконтування i є нижчім рівня інфляції r

$$i<r. \tag{11}$$

Для перебування ДКФС, яка експлуатується в умовах (11), в стані S_{on} необхідно закласти на етапі її проектування такий обсяг ресурсів *C*, з яким для значення імовірності переходу ДКФС в стан S_{off} внаслідок реалізації негативного впливу $\pi(C)$ виконувалася б нерівність $\pi(C)<(-\lambda+\ln\gamma)/\mu q$.

Тепер опишемо поведінку ДКФС в ситуації, коли умова (11) не виконується. Перепишемо вираз (9) таким чином:

$$\beta^{-}_{\lim}(C) = \frac{w_0(1-q\pi(C))}{C(\lambda-\ln\gamma)/\mu+q(C+d_0)\pi(C)}. \tag{12}$$

Отримаємо аналітичну форму похідної від параметра (12)

$$\frac{d\beta_{\lim}^{-}(C)}{dC}=\frac{-w_0 q\left(C+d_0+\left(C\left(\lambda-\ln\gamma\right)\right)/\mu\right)\pi'(C)}{\left(\left(C\left(\lambda-\ln\gamma\right)\right)/\mu+q\left(C+d_0\right)\pi(C)\right)^2}+\frac{w_0 q\left(q\pi(C)+\left(\lambda-\ln\gamma\right)/\mu-1\right)-\left(\lambda-\ln\gamma\right)/\mu}{\left(\left(C\left(\lambda-\ln\gamma\right)\right)/\mu+q\left(C+d_0\right)\pi(C)\right)^2}. \quad (13)$$

З виразу (13) видно, що чисельник функції $d\beta_{\lim}^{-}(C)/dC$ є квадратичною функцією відносно параметра $\pi(C)$. Отже, якщо один з коренів функції (13) належить до інтервалу $[0,1]$, то екстремум функції $\beta_{\lim}^{-}(C)$ існує. Подамо це твердження аналітично

$$q^2\pi^2+\left(\left(\left(\lambda-\ln\gamma\right)/\mu-1\right)\pi-q\left(d_0+C+\left(C\left(\lambda-\ln\gamma\right)\right)/\mu\right)\pi'-\left(\lambda-\ln\gamma\right)/\mu=0. \quad (14)$$

Для спрощення розв'язку рівняння (14) припустимо, що залежність $\pi(C)$ має експоненціальний характер $\pi(C)=\exp(-\xi C)$, де коефіцієнт $\xi>0$ характеризує ефект від закладених в кібербезпеку ДКФС ресурсів C. Доопрацюємо вираз (14) з урахуванням інтерпретації функції $\pi(C)$

$$q^2\pi^2-\pi\left(1-\left(\lambda-\ln\gamma\right)/\mu-q\xi\left(\lambda-\ln\gamma\right)/\mu=0. \quad (15)$$

Запишемо вираз (15) в компактній формі

$$q^2\pi^2-s\pi-b=0, \quad (16)$$

де $s=1-\left(\lambda-\ln\gamma\right)/\mu-q\left(d_0+C+\left(C\left(\lambda-\ln\gamma\right)\right)/\mu\right)\xi$; $b=\left(\lambda-\ln\gamma\right)/\mu$. Очевидно, що додатний корінь такого рівняння визначається як

$$\pi=\left(s+\sqrt{s^2+4bq^2}\right)/2q^2. \quad (17)$$

Орієнтуючись на факт існування та значення параметра π, визначеного за виразом (17), можна оцінити на скільки обсяг ресурсів, закладених на етапі проектування ДКФС в її кіберімунний потенціал, *C* відповідає реальному рівню агресивності кіберпростору $\beta(t)$, де ДКФС експлуатується.

Враховуючи вихідні положення цього дослідження, можна стверджувати: якщо негативний вплив, що реалізується, не ідентифікований, то його діяльність гарантовано спричинить перехід ДКФС в стан S_{off}. До того ж, закладений на етапі проектування ДКФС кіберімунний потенціал дозволяє у випадку ідентифікації негативного впливу нейтралізувати його з імовірністю q. Вищенаведена аналітична концепція не враховує того, що негативний вплив може бути ідентифікований неправильно (похибка другого роду), тому введемо стохастичний параметр *f*, який характеризує імовірність того, що реалізовуваний негативний вплив буде правильно ідентифікований ДКФС. З урахуванням цього параметра кіберфізична система може перейти в стан S_{off} внаслідок негативного впливу якщо:

– негативний вплив не ідентифіковано — $1-f$;

– негативний вплив ідентифіковано, але не нейтралізовано — πf.

З урахуванням цієї інформації перепишемо рівняння (2)—(4)

$$\frac{dp_0(t)}{dt}=-p_0(t)\cdot\left(q\mu(t)\left(1-f\left(1-\pi\right)\right)+\lambda(t)\right); \quad (18)$$

$$\frac{dW(t)}{dt}=p_0(t)\cdot\left(1-q+qf\left(1-\pi\right)\right)\mu(t)w(t); \quad (19)$$

$$\frac{dR(t)}{dt}=p_0(t)\cdot q\left(1-f\left(1-\pi\right)\right)\mu(t)d(t). \quad (20)$$

Введення параметра f є підставою для переосмислення способу врахування втрат d_0, яких зазнає ДКФС в разі передчасного переривання процесу експлуатації. Введемо такі показники:
d_1 — втрати, спричинені реалізацією негативного впливу, в наслідок якого ДКФС перейшла в стан S_{off} з дотриманням протоколу функційної безпеки; d_2 — втрати, спричинені реалізацією

негативного впливу, в наслідок якого ДКФС неконтрольовано перейшла в стан S_{off} (аварійна ситуація). Введемо ці показники в рівняння (20)

$$\frac{dR(t)}{dt} = p_0(t)\cdot q\left(f(1-\pi)d_1 + (1- f + \pi f)d_2\right)\mu(t)\gamma^t. \quad (21)$$

Модель (18), (19), (21) все ще не повністю описує реальний процес експлуатації ДКФС в агресивному кіберфізичному просторі. Зокрема, досліджуючи питання ідентифікації негативного впливу, не можна ігнорувати імовірність виникнення похибок першого роду, тобто ситуацій, коли цільова кіберімунна реакція є наслідком ідентифікації негативного впливу, який насправді не реалізовувався. При цьому слід врахувати, що під час кіберімунної реакції цільове використання ДКФС неможливе. Для врахування щойно описаної ситуації розширимо простір станів досліджуваної системи: $S = \left\{S_{on}, S_1, S_2, S_{off}\right\}$, де S_{on} — це стан готовності, перебуваючи в якому ДКФС, що функціонує, очікує на вхідний запит, який надходить з інтенсивністю $\mu(t)$. Імовірність перебування ДКФС в стані S_{on} характеризується параметром $p_0(t)$; S_1 — це стан опрацювання отриманого запиту, що здійснюється з інтенсивністю $v(t)$. Імовірність перебування ДКФС в стані S_1 характеризується параметром $p_1(t)$; S_2 — це стан активної кіберімунної реакції, коли з інтенсивністю $\phi(t)$ виконується цільовий протокол політики безпеки. Імовірність перебування ДКФС в стані S_2 характеризується параметром $p_2(t)$; S_{off} — це стан, перебуваючи в якому ДКФС не функціонує. Імовірність перебування ДКФС в стані S_{off} характеризується параметром $p_3(t)$. Стани S_{on} і S_1 — функціональні, адже перебуваючи в них ДКФС реалізує своє цільове призначення. Відповідно стани S_2 і S_{off} — не функціональні.

Нехай негативні впливи реалізуються з інтенсивністю $\eta(t)$. Припустимо, що зафіксований негативний вплив є імітацією. Охарактеризуємо таку подію імовірністю l_0. Позначимо ідентифікатором f_0 імовірність правильної ідентифікації імітації негативного впливу, а ідентифікатором f_1 — імовірність правильної ідентифікації негативного впливу. В сумі ці параметри характеризують імовірність правильної ідентифікації негативної активності. Не змінюватимемо інтерпретацію інтенсивності відмов ДКФС як $\lambda(t)$ та імовірності переходу системи в нефункціональний стан в наслідок реалізації негативного впливу як π. Обмежена простором станів S динаміка процесу експлуатації ДКФС визначається рівняннями

$$\frac{dp_0(t)}{dt} = p_0(t)\cdot\left(-\mu(t)\right) + p_1(t)\cdot v(t); \quad (22)$$

$$\frac{dp_1(t)}{dt} = p_0(t)\cdot\mu(t) + p_2(t)\cdot\phi(t)\left(1-\pi(1-l_0)\right) - p_1(t)\cdot\left(\lambda(t) + v(t) + \eta(t)(1- f_0 l_0)\right); \quad (23)$$

$$\frac{dp_2(t)}{dt} = p_2(t)\cdot\left(-\phi(t)\right) + p_1(t)\cdot\eta(t)\left(f_1(1-l_0) + l_0(1- f_0)\right); \quad (24)$$

$$\frac{dp_3(t)}{dt} = p_2(t)\cdot\left(\phi(t)\pi(1-l_0)\right) + p_1(t)\cdot\left(\lambda(t) + \eta(t)(1- f_1)(1-l_0)\right). \quad (25)$$

Визначимо аналоги рівнянь (3) і (4) з урахуванням факту існування рівнянь (22)—(25)

$$dW(t)/dt = p_1(t)\cdot w(t)v(t); \quad (26)$$

$$\frac{dR(t)}{dt} = d_1\cdot p_2(t)\phi(t)(1- f_1)(1-l_0)\gamma^t + d_2\cdot\left(p_1(t)\eta(t)(1-\pi)(1-l_0) + p_2(t)\phi(t)\pi(1-l_0)\right)\gamma^t. \quad (27)$$

Рівняння (23) і (26) можна спростити таким чином, припускаючи, що ДКФС експлуатується постійно:

$$\frac{dp_1(t)}{dt} = p_1(t)\cdot -\left(\eta(t)(1- f_0 l_0)+\lambda(t)\right)+ p_2(t)\cdot\phi(t)\left(1-\pi(1-l_0)\right);$$

$$dW(t)/dt = p_1(t)\cdot w(t).$$

Таке припущення не впливає на рівняння (24), (25), (27).

Постановка і результати експерименту

Строга коректність і зворотність аналітичних перетворень свідчать на користь адекватності поданого в розділі 3 математичного апарату. Зрештою, залишилось його випробувати в реальних умовах. Згідно з попередньою домовленістю, автори мали змогу апробувати розроблений математичний апарат, описавши процес експлуатації реальної кіберфізичної системи Ситуаційного центру департаменту кіберфізичних технологій Вінницької міської ради. Ця кіберфізична система функціонує з 2018 р. і постійно розвивається в напрямку вдосконалення впроваджених сервісів та додавання нових. Зокрема, кіберфізична система Ситуаційного центру здійснюється управління світлофорами на дорогах міста та підтримує безперебійну експлуатацію дата-центру, в якому зберігається потік мультимедіа даних від понад 1000 розташованих у місті відеокамер. Доступ до зібраної конфіденційної інформації мають лише авторизовані співробітники Служби безпеки України, Національної поліції України, Вінницької міської ради тощо. Зважаючи на інтенсивність кіберфізичного обміну та характер кіберфізичних ресурсів, питання моделювання процесу експлуатації цієї ДКФС є надзвичайно актуальним.

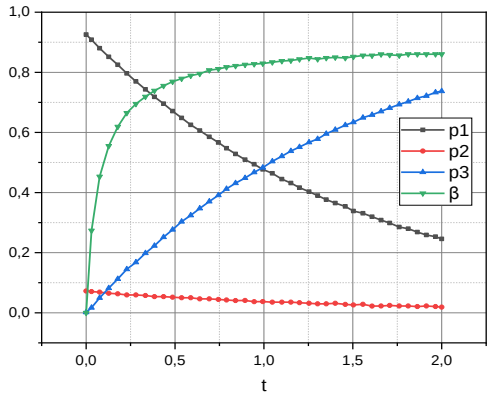

Рис. 1. Емпіричні залежності $\{p_1, p_2, p_3\} = f(t)$

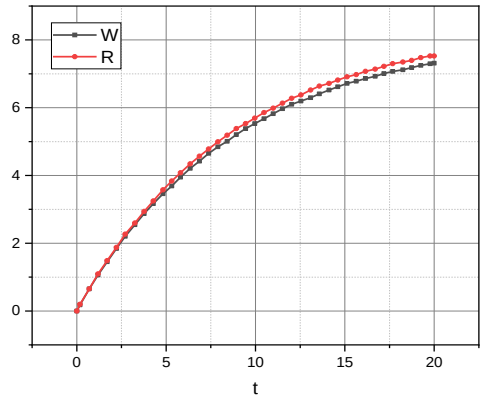

Рис. 2. Емпіричні залежності $\{W, R\} = f(t)$

Щоб цей розділ був достатньо компактним, моделювання ДКФС здійснюватимемо в просторі станів $S = \left\{S_{on} = \{S_{on}, S_1\}, S_{off} = \{S_2, S_{off}\}\right\}$. Аналіз логів неперервної експлуатації ДКФС з 01.09.2019 р. по 01.09.2021 р. в контексті вибраної конфігурації простору дозволив визначити такі значення усталених параметрів створюваної моделі: $\lambda = 10^{-5}$; $\pi = 0{,}01$; $r = 0{,}05$; $i = 0{,}1$; $\eta = 5$; $\phi = 50$; $f_0 = f_1 = 0{,}99$; $d_0 = 0{,}1$; $d_1 = 10$; $l_0 = 0{,}2$; $w_0 = 1$. Як вихідне значення візьмемо $C = 1$. Підставивши ці параметри у вирази (23)—(26), здійснено імітаційне моделювання залежностей $\{p_1, p_2, p_3\} = f(t)$ $\{W, R\} = f(t)$ для ДКФС. Відповідні результати показано графіками на рис. 1.

Використовуючи розрахунки, результати яких візуалізовано на рис. 1, на основі виразів (26) і (27) для ДКФС розраховані залежності $\{W, R\} = f(t)$, де W — накопичуваний параметр ефективності експлуатації ДКФС, а R — супутній ризик від її експлуатації. Відповідні графіки показані на рис. 2.

Нарешті, центральним питанням цього дослідження є встановлення факту: чи достатні здійснені на етапі проектування ДКФС капіталовкладення в її кіберімунну систему з огляду на рівень агресивності кіберпростору, представлений значенням параметра π? Для відповіді на це питання проведено серію експериментів з метою розрахунку залежностей $\beta = f(\pi)$, коли $\pi(C) = \text{const}$ і $\pi(C) = \exp(-C)$. Нагадаємо, що $\beta = f(W, R, C)$ є узагальненим коефіцієнтом ефективності ДКФС щодо виконання нею цільового призначення в реальних умовах експлуатації.

Зважаючи, що для цієї ДКФС умова (11) не виконувалася, то залежності $\beta = f(\pi)$ розраховувалися за виразом (13). Також актуальною є об'єктивна інформація щодо розрахунку для ДКФС

залежності $\beta = f(1-f_1)$, де f_1 — імовірність правильної ідентифікації негативного впливу. Тобто, ця залежність характеризує спроможність кіберімунної системи ДКФС нейтралізувати виявлений, але неправильно ідентифікований негативний вплив. Графік, який репрезентує розраховану для ДКФС залежність $\beta = f(1-f_1)$, коли $\pi = 0{,}005$, показаний на рис. 3.

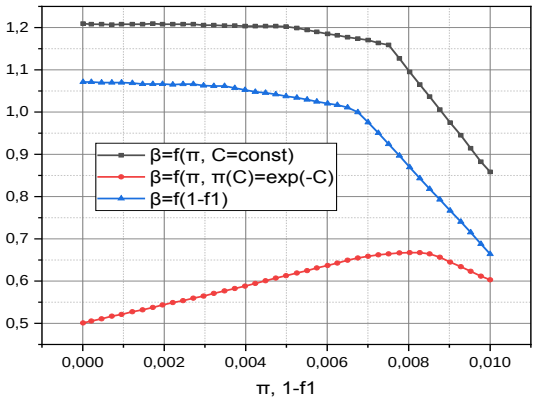

Рис. 3. Емпіричні залежності $\beta = f(\pi, C = \text{const})$; $\beta = f(\pi, \pi(C) = \exp(-C))$; $\beta = f(1-f_1)$

Розпочнемо обговорення з аналізу графіків на рис. 1. Нагадаємо, що параметри $p_1(t)$, $p_2(t)$, $p_3(t)$ характеризують імовірності перебування ДКФС в момент часу t в стані S_1, S_2, S_{off} відповідно. З них функціональним є стан S_1. Стан S_2 відповідає активній кіберімунній реакції, а стан S_{off} описує ситуацію, коли ДКФС передчасно виведена з експлуатації в наслідок реалізації негативного фактору. Залежності $\{p_1, p_2, p_3\} = f(t)$ зі зростанням значення t однозначно відтворюють реальну динаміку процесу експлуатації ДКФС: $p_2(t)$ спадає, а $p_2(t)$ навпаки зростає. Те, що при цьому $p_3(t)$ повільно спадає свідчить про надлишковість вкладених в кібербезпеку ДКФС ресурсів C. Втім, в умовах зростання імовірності негативного впливу коефіцієнт ефективності експлуатації ДКФС β все одно зростає, адже графік $p_2(t)$ також є зростальним. Підтверджують достатність вкладених в кібербезпеку ресурсів і показані на рис. 2 залежності $\{W, R\} = f(t)$. Це твердження правильне, адже динаміка зростання накопичуваного показника ефективності експлуатації ДКФС W випереджає динаміку зростання характеристики ризику від її експлуатації R. Загалом, нелінійний експоненційний характер залежностей з рис. 1 і 2 підтверджує коректність припущення (5), що ефективність експлуатації ДКФС $(\beta = f(t))$ зростає попри факт, що за результатами вихідних умов експерименту нерівність (11) не виконується. Показані на рис. 1 і 2 результати імітаційного моделювання повністю відповідають емпіричному досвіду експлуатації ДКФС, що дозволяє визнати розроблений математичний апарат адекватним.

Приділимо увагу рис. 3. Видно, що з перетином графіком функції $\beta = f(1-f_1)$ рівня $\approx 0{,}007$ значення коефіцієнта ефективності експлуатації ДКФС β починає швидко спадати. Це свідчить про те, що обсяг закладених в кібербезпеку ресурсів C вичерпано. Таке твердження корелює з динамікою, яку демонструє графік $\beta = f(\pi, C = \text{const})$ і загалом підтверджує коректність створеного математичного апарату. Нарешті, видимий екстремум на графіку $\beta = f(\pi, \pi(C) = \exp(-C))$ та сама форма цієї залежності задовольняє логіці математичних концепцій, втілених у вираз (17). Проте, очевидно, що питання визначення оптимального обсягу ресурсів C, закладених на етапі проектування ДКФС в її кібербезпеку, слід досліджувати в повнорозмірному параметричному просторі $\{\pi, l_0, f_0, f_1\}$, що є перспективним напрямом подальших досліджень.

Висновки

Кіберфізичні системи призначені для забезпечення первинної потреби сучасної людини — доступу до даних. Дослідження, спрямовані на підвищення якісних показників реалізації сервісів таких систем є беззаперечно актуальними.

Розроблено математичний апарат для моделювання процесу експлуатації кіберфізичної системи в умовах агресивного зовнішнього кіберпростору, для врахування якого передбачено відповідний параметр. На відміну від аналогів, моделювання здійснюється в параметричному просторі індикаторів безвідмовності, функційної безпечності та таких економічних показників як прибуток від цільового використання досліджуваної системи та коефіцієнти інфляції та дисконтування. Узагальнювальним параметром в математичному апараті є коефіцієнт ефективності експлуатації дос-

ліджуваної кіберфізичної безпеки, в якому враховуються накопичуваний параметр ефективності експлуатації кіберфізичної системи, супутній ризик від її експлуатації та обсяг ресурсів, вкладених в заходи кібербезпеки на етапі її проектування. Аналітично описаний зв'язок цього коефіцієнта з імовірністю переходу кіберфізичної системи в нефункціональний стан внаслідок реалізації негативного впливу попри супротив кіберімунної реакції. Математичний апарат розвинуто в напрямку врахування похибок першого та другого роду за ідентифікації негативного впливу кіберфізичною системою. Окремо досліджено випадок кіберімунної реакції на імітацію негативного впливу. Формалізовано пошук екстремального значення коефіцієнта ефективності експлуатації кіберфізичної системи від обсягу вкладених ресурсів в заходи її кібербезпеки та враховано характеристичні параметри кіберпростору, в якому досліджувана система експлуатується. Дослідження реальної кіберфізичної системи Ситуаційного центру департаменту кіберфізичних технологій Вінницької міської ради довело адекватність запропонованого математичного апарату.

Подальші дослідження планується спрямувати на деталізацію параметричного простору поставленої задачі пошуку екстремального значення коефіцієнта ефективності експлуатації ДКФС.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] S. Colabianchi, F. Costantino, G. Di Gravio, F. Nonino, and R. Patriarca, "Discussing resilience in the context of cyber physical systems," *Computers & Industrial Engineering*, 2021. https://doi.org/10.1016/j.cie.2021.107534 .

[2] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review*, vol. 35, February, 2020, https://doi.org/10.1016/j.cosrev.2019.100219 .

[3] P. G. George, and V. R. Renjith, "Evolution of Safety and Security Risk Assessment methodologies towards the use of Bayesian Networks in Process Industries," *Process Safety and Environmental Protection*, 2021. https://doi.org/10.1016/j.psep.2021.03.031.

[4] Li Zhang, and Vrizlynn L. L. Thing, "Three decades of deception techniques in active cyber defense – Retrospect and outlook," *Computers & Security*, vol. 106, pp. 10228, July 2021. https://doi.org/10.1016/j.cose.2021.102288 .

[5] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Computers & Security*, 2020. https://doi.org/10.1016/j.cose.2019.101677 .

[6] X. Yuan et al., "Decoupled reliability-based optimization using Markov chain Monte Carlo in augmented space," *Advances in Engineering Software*, 2021. https://doi.org/10.1016/j.advengsoft.2021.103020 .

[7] Q. Zhang, and Y. Liu, "Reliability evaluation of Markov cyber–physical system oriented to cognition of equipment operating status," *Computer Communications*, 2022. https://doi.org/10.1016/j.comcom.2021.10.004 .

[8] B. Wu, and L. Cui, "Reliability of multi-state systems under Markov renewal shock models with multiple failure levels," *Computers & Industrial Engineering*, 2020. https://doi.org/10.1016/j.cie.2020.106509 .

[9] O. Bisikalo, D. Chernenko, O. Danylchuk, V. Kovtun, and V. Romanenko, "Information Technology for TTF Optimization of an Information System for Critical Use that Operates in Aggressive Cyber-Physical Space," *IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020. https://doi.org/10.1109/picst51311.2020.9467997 .

[10] O. V. Bisikalo, V. V. Kovtun, O. V. Kovtun, and O. M. Danylchuk, "Mathematical Modeling of the Availability of the Information System for Critical Use to Optimize Control of its Communication Capabilities," *SWCC*, 2021. https://doi.org/10.2174/2210327910999201009163958 .

Рекомендована кафедрою комп'ютерних систем управління ВНТУ

Стаття надійшла до редакції 13.12.2023

Биков Микола Максимович — канд. техн. наук, професор, професор кафедри комп'ютерних систем управління, e-mail: mbykov123@ukr.net ;

Грищук Тетяна Вікторівна — канд. техн. наук, доцент, доцент кафедри комп'ютерних систем управління, e-mail: tetiana.gryshchuk@vntu.edu.ua ;

Ковалюк Олег Олександрович — канд. техн. наук, доцент, доцент кафедри комп'ютерних систем управління, e-mail: oleh.kovalyuk@vntu.edu.ua ;

Ковтун В'ячеслав Васильович — д-р техн. наук, професор, завідувач кафедри комп'ютерних систем управління, e-mail: kovtun_v_v@vntu.edu.ua ;

Юхимчук Марія Сергіївна — д-р техн. наук, доцент, професор кафедри комп'ютерних систем управління, e-mail: umcmasha@gmail.com

M. M. Bykov[1]
T. V. Gryshchuk[1]
O. O. Kovaliuk[1]
V. V. Kovtun[1]
M. S. Yukhymchuk[1]

Model of Cyber-Physical System Operation Under the Impact of Negative External Factors

[1]Vinnytsia National Technical University

The article presents a mathematical tool for modeling the process of cyber-physical system operation under the impact of negative external factors, which is taken into account by the corresponding parameter. Unlike analogues, the model of the researched process is formalized in the parametric space of failure-free, functional safety and a number of economic indicators. The generalizing parameter in the presented mathematical tool is the efficiency coefficient, which takes into consideration the cumulative parameter of the cyber-physical system operation efficiency, the accompanying risk from its operation and the amount of resources invested in cyber security measures at the stage of designing the target system. The relationship of this coefficient with the probability of the transition of the cyber-physical system into a non-functional state as a result of the realization of a negative impact despite the opposition of cyber security means is analytically described. The mathematical tool was developed in the direction of taking into account errors of the first and second kind when identifying a negative impact by means of cyber security. The case of the reaction of cyber security tools to the imitation of a negative impact was separately investigated. The search for the extreme value of the efficiency coefficient based on the amount of resources invested in cyber security measures and taking into account the characteristic parameters of the space in which the target cyber-physical system is operated is formalized. The study of the real cyber-physical system of the Situation Center of the Department of Cyber-Physical Technologies of the Vinnytsia City Council showed the adequacy of the proposed mathematical tool.

Keywords: cyber-physical system, negative factor, operation process, mathematical model, fail-safe, functional safety, efficiency.

Bykov Mykola M. — Cand. Sc. (Eng.), Professor, Professor of the Chair of Computer Control Systems, e-mail: mbykov123@ukr.net ;

Gryshchuk Tetiana V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Computer Control Systems, e-mail: tetiana.gryshchuk@vntu.edu.ua ;

Kovaliuk Oleh O. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Computer Control Systems, e-mail: oleh.kovalyuk@vntu.edu.ua ;

Kovtun Viacheslav V. — Dr. Sc. (Eng.), Professor, Head of the Chair of Computer Control Systems, e-mail: kovtun_v_v@vntu.edu.ua ;

Yukhymchuk Maria S. — Dr. Sc. (Eng.), Associate Professor, Professor of the Chair of Computer Control Systems, e-mail: umcmasha@gmail.com