DOI: 10.18372/2410-7840.21.13543
УДК 602.1:519.85:53.082.9:616-07

ПРО МОДЕЛЬ КІБЕР-ФІЗИЧНОЇ СИСТЕМИ З АТАКАМИ СТАНУ ТА ВИМІРЮВАНЬ НА ОСНОВІ СТОХАСТИЧНИХ РІЗНИЦЕВИХ РІВНЯНЬ

Василь Марценюк, Андрій Сверстюк

Статтю присвячено питанням моделювання кібер-фізичних систем з урахуванням інформаційних загроз. Проаналізовано принципи організації структури та надійного функціонування досліджуваних систем. Наведено концептуальну модель кібер-фізичних систем з урахуванням інформаційних загроз. У роботі запропоновано конструктивний алгоритм для пошуку оцінки в кіберфізичній моделі при атаках на стан та спостереження на основі вимірювання показників системи. Модель представлена у вигляді нестаціонарної дескрипторної системи, яка включає диференціальні рівняння для змінних стану вузла та алгебраїчні рівняння для вимірювань. Змінні стану та вимірювання вважаються випадковими векторами. Використано інформаційний критерій, щоб знайти оптимальну оцінку скалярного добутку, який характеризує стан системи. Алгоритм грунтується на зведенні задачі оцінювання до задачі оптимального керування. Отримано значення середньоквадратичної похибки, яка не залежить від атак. Оцінювання виконувалося у вигляді скалярного добутку, що включає вектор вимірювань. Запропоновано алгоритм побудови оптимальної оцінки для скалярного добутку, що включає стан мережевої моделі під час атаки. Взаємна інформація між випадковими векторами використовувалася як критерій якості для оптимізації. Оцінювання виконувалося у вигляді скалярного добутку, що включає вектор вимірювань. Розглядаючи ефекти атак на цю оцінку, слід зазначити, що побудована оцінка залежить від таких атак лише через множник. Середньоквадратичної похибка такої оцінки не залежить від атаки. Причиною відсутності впливу атаки на середньоквадратичну похибку є квадратична форма множин, які вибрані для атак стану. Дане припущення дає змогу застосувати апарат лінійно-квадратичної оптимізації, що зводить проблему оцінювання до задачі оптимального керування. Одержані результати проілюстровано на чисельному прикладі для стану системи без шуму і з атаками та стану системи з шумом і атаками. При цьому було використано трьохвузлову кіберфізичну систему, яка може використовуватися для планування технічного обслуговування та оптимізованого управління для досягнення більш високої загальної продуктивності та безпеки досліджуваних систем.

Ключові слова: *кібер-фізична система, стохастичні різницеві рівняння, задача оптимального оцінювання, мережева модель..*

Вступ. Кібер-фізичні системи (КФС) – це системи, що складаються з різних фізичних (природних і промислових об'єктів), штучних підсистем, і керовані з використанням зворотного зв'язку від різних датчиків (сенсорів) [1]. В основу функціонування КФС закладений принцип інтеграції обчислювальних і фізичних процесів, тобто фізичні об'єкти стають частиною системи [2].

З технічної точки зору КФС мають багато спільного зі структурами типу грід, реалізованими за допомогою інтернету речей (Internet of Things, IoT), Індустрії 4.0 (Industry 4.0), промислового інтернету речей (Industrial Internet), міжмашинної взаємодії (Machine-to-Machine, M2M), туманного і хмарного комп'ютингу (fogi cloud computing).

Кібер-фізичні системи виникають через тісну інтеграцію фізичних процесів, обчислювальних ресурсів та можливостей комунікації. Точніше, процесори контролюють і контролюють фізичні процеси за допомогою датчиків і мереж активаторів. Прикладами кібер-фізичних систем є транспортні мережі, мережі виробництва та розподілу електроенергії, водорозподільні та газорозподільні мережі, а також вдосконалені системи зв'язку. Через вирішальну роль КФС у повсякденному житті необхідно забезпечувати їм безпеку.

Окрім атак на фізичну інфраструктуру, кібер-фізичні системи також схильні до кібератак на рівні управління даними та зв'язку. Недавні дослідження та реальні інциденти продемонстрували нездатність існуючих методів безпеки забезпечити безпечну та надійну функціональність кібер-фізичних інфраструктур від непередбачених збоїв та зовнішніх атак [3-6].

Аналіз уразливостей кібер-фізичних систем до зовнішніх атак отримав все більше уваги в останні роки [7-9]. Загальним підходом було вивчення впливу конкретних атак на окремі системи. Наприклад, в [10] вводиться відмова в обслуговуванні атаки на мережеву систему управління з використанням відповідної комп'ютерної програми. Атаки обману відносяться до можливості компрометації цілісності контрольних пакетів або вимірювань, і вони відкидаються шляхом зміни поведінки давачів та пристроїв керування. Атаки відмов при обслуговуванні КФС перешкоджають каналам зв'язку та ставлять під загрозу доступність

ресурсів. В [11] вводяться помилкові атаки введення даних проти статичних оцінок стану. Помилкові атаки ввведення даних є специфічними атаками обману в контексті статичних оцінювачів. У роботі [14] наведено вплив атаки шляхом захоплення сенсорів, запису показань протягом певного часу і повторення таких показання при введенні в систему сигналу, невідомого зловмиснику. В [15] досліджено вплив прихованих атак на мережеві системи управління. Зокрема, параметризована структура КФС дає змогу прихованому агенту змінювати поведінку фізичної установки, залишаючись невизначеною від вихідного контролера. У роботі [16] досліджується проблема стійкого управління, в якій керуючі пакети, що передаються по мережі, пошкоджуються зловмисником. Останнім часом досліджено проблему оцінки стану лінійної системи з пошкодженими результатами вимірювання [17]. Більш точно, характеризується максимальне число несправних датчиків, які можна допустити, і запропоновано алгоритм декодування для виявлення пошкоджених вимірювань. Значна увага приділена питанням безпеки деяких специфічних КФС, серед яких енергетичні мережі [12], [18], лінійні мережі з несправними компонентами [6] та водопровідні мережі [13], [15].

Мета роботи. Запропонувати безпекову модель КФС на основі дескрипторної системи. Розробити алгоритм побудови оптимальної оцінки стану мережевої моделі КФС з урахуванням атак.

1. Концептуальна модель архітектури КФС.

Можна припустити, що інфраструктура КФС є фабрикою по обробці інформації, що вписується в інформаційно-технологічну концепцію досліджуваних систем. Це велика кількість пристроїв з вбудованими сенсорами, процесорами і засобами зберігання даних. При цьому використовується інтеграція, що дає змогу досягти найбільшого ефекту шляхом об'єднання окремих компонентів у велику систему.

Інфраструктура КФС складається з наступних основних компонентів, таких як комунікаційна мережа, обчислювальні ресурси, зберігання даних, інформаційні ресурси, технології інтелектуального аналізу [19], [20].

Виходячи із вищенаведеної інформації, концептуальна модель архітектури повинна складається з п'яти рівнів, а саме:

1. Розумне з'єднання. На цьому рівні збираються дані зі smart давачів різного призначення.

2. Перетворення даних. На цьому рівні обробляються первинні дані з використанням різних алгоритмів.

3. Кібер або віртуальний рівень. Цей рівень використовується як хаб з метою виконання складної аналітики для формування рекомендацій для кращого використання певних блоків, вузлів, елементів.

4. Рівень діагностування. Система використовує on-line моніторинг, щоб діагностувати свої власні потенційні збої на основі адаптивного навчання і виходячи з історії оцінок стану.

5. Рівень прийняття рішень. На цьому рівні здійснюється зворотний зв'язок від кіберпростору до фізичного простору для застосування до системи, що діагностується коригувальних впливів, які були прийняті на попередньому рівні.

Як випливає з моделі, кожен рівень окремо, поряд з виконанням своїх основних функцій, вимагає забезпечення безпеки. Загальна політика безпеки включає в себе як безпеку кожного рівня, так і системи в цілому.

Запропонована в наступному розділі модель КФС призначена для використання на рівнях діагностування та прийняття рішень.

2. Модель кіберфізичної системи.

В даній роботі використано загальний підхід, який запропонований у [21] для моделювання складних мереж у нестаціонарному випадку. Мета полягає в побудові алгоритму оцінки розв'язків задачі. Спостерігаємо деяку складну мережу в певні моменти часу $t = \overline{0,T-1}$. Згідно з підходом роботи [21] мережа представляється множиною неорієнтованих графів $G(t) := (V, \varepsilon(t))$, $t = \overline{0,T-1}$, де $V := \{1,...,n\}$ та $\varepsilon(t) \subseteq V \times V$, $t = \overline{0,T-1}$ – вершини та множини ребер, відповідно. У нестаціонарному випадку сукупність ребер змінюється разом із часом. Наведемо наступні припущення для будь-якого дискретного моменту часу $t = \overline{0,T-1}$.

Нехай для будь-якого $t \in \overline{0,T-1}$ $a_{ij}(t) \in R$ – вага, пов'язана з ребром $(i,j) \in \varepsilon(t)$. Введемо матриці спряженості для графів $G(t)$, що містять відповідні ваги, таким чином, що $A(t) = A^{\mathrm{T}}(t) = [a_{ij}(t)]$, де $a_{ij}(t) = 0$.

Крім того, розглядається деякий "білий шум", що впливає на вузли мережі в момент часу t. Тобто маємо послідовність випадкових векторів $\{\xi(t), t = \overline{0,T-1}\}$, які є гаусівськими випадковими векторами.

Поєднаємо дійсне значення (стан) з кожним вузлом. Об'єднаємо набір станів вузлів у вектор (стану мережі) і визначимо відображення x: $N \geq 0 \to R^n$ для опису еволюції стану мережі з часом (мережева динаміка). Розглянемо дискретну нестаціонарну мережеву динаміку, що описується рівнянням

$$x(t+1) = A(t)x(t) + \xi(t), x(0) = x_0, \quad (1)$$

де $A(t) \in R^{n\times n}$, $t = \overline{0, T-1}$ відомі дійснозначні матриці; x_0 – гаусівський випадковий вектор.

Модель кібер-фізичної системи розглядається на основі лінійної нестаціонарної дескрипторної системи

$$\begin{aligned} x(t+1) &= A(t)x(t) + Bu(t) + \xi(t), x(0) = x_0, \\ y(t) &= C(t)x(t) + Du(t) + \eta(t), t = \overline{0, T-1}, \end{aligned} \quad (2)$$

де $x(t) \in R^n$, $y(t) \in R^p$, $A(t) \in R^{n\times n}$, $B \in R^{n\times m}$, $C(t) \in R^{p\times n}$ і $D \in R^{p\times m}$. У рівняннях (2) розглядається деякий "білий шум", що впливає на вимірювані вектори, а саме $\{\eta(t), t = 0, T-1\}$, які є гаусівськими випадковими векторами. Вхідні величини $Bu(t)$ та $Du(t)$ є невідомими сигналами, що описують завади, які впливають на мережу. Саме вони відображають «збій» роботи системних компонентів. Ці порушення моделюють ефект атаки на кіберфізичну систему (див. [22] для повного опису моделі атак).

Для зручності позначень та без обмеження загальності, ми припустимо, що згідно [22] кожен стан і вихідна змінна можуть бути незалежно атаковані. Таким чином, ми можемо представити матриці у вигляді $B = [I, 0]$ і $D = [0, I]$, де I – тотожня матриця, 0 – нульова матриця відповідних розмірів і, звідси, $u(t) = [u_x(t)^T, u_y(t)^T]^T$. Отже, атака $(Bu(t), Du(t)) = (u_x(t), u_y(t))$ може бути класифікована як атака стану, що впливає на динаміку системи та, у випадку атаки, збурює також вектор вимірювань. Повна модель кіберфізичної системи з урахуванням атак, включаючи монітори та атаки різних типів, описана в [22].

У кінцевому випадку отримуємо таку дескрипторну систему

$$\begin{aligned} x(t+1) &= A(t)x(t) + u_x(t) + \varepsilon(t), x(0) = x_0, \\ y(t) &= C(t)x(t) + u_y(t) + \eta(t), t = \overline{0, T-1}. \end{aligned} \quad (3)$$

Припустимо, що послідовності випадкових векторів $\{\xi(t), t = \overline{0, T-1}\}$, $\{\eta(t), t = \overline{0, T-1}\}$ є гаусівськими некорельованими між собою і між випадковим вектором x_0.

Припустимо, не обмежуючи загальності, що

$$\mathrm{E}\,\xi(t) = 0, \mathrm{E}\,\xi(t) = 0, \mathrm{E}\,x_0 = m_0,$$

$$\mathrm{E}[x_0 x_0^{\mathrm{T}}] = R_0, \quad \mathrm{E}[\xi(t)\xi^{\mathrm{T}}(t)] = R(t), \quad t = \overline{0, T-1}.$$

Вважаємо, що u_x, u_y послідовності визначених векторів.

Припустимо, що

$$\eta(t) \in G = \{\eta(t), t = \overline{0, T-1} : \sum_{i=0}^{T-1} E\eta^{\mathrm{T}}(t)Q(t)\eta(t) \leq 1,$$

де $Q(t)$ – задані додатньовизначені матриці відповідної розмірності.

Тобто множина G є гіпереліпсоїдом. Для обчислень використовуватимемо тотожність $\mathrm{E}\,\eta^{\mathrm{T}}Q\eta = QK_\eta$, де $K_\eta = \mathrm{E}\eta^{\mathrm{T}}\eta$ – коваріаційна матриця.

Припустимо, що $u_x(t) \in G_1(t), u_y(t) \in G_2(t)$, де $G_1(t), G_2(t)$ – задані множини. При цьому нехай $G_1(t)$ має квадратичну форму

$$G_1(t) = \{\upsilon(t) : \upsilon^{\mathrm{T}}(t)Q_1(t)\upsilon(t) \leq 1, \quad t = \overline{0, T-1}\}.$$

В роботі [22] модель на основі рівнянь дескрипторної системи (3) застосовано для дослідження атак стану електромережі, а в роботі [11] при дослідженні атак на виходи 14 ліній електромереж. В роботі [23] на основі досліджуваної моделі (3) розглядається мережева система водопостачання при атаках, як на стан, так і на вимірювання.

3. Проблема оцінювання з інформаційним критерієм.

Однією з найважливіших задач для (3) є проблема оцінювання. Значне число досліджень було присвячене проблемі оцінки стану для стохастичних систем.

Робота [24] була однією з перших, метою якої було вивчення проблеми фільтрації з точки зору теорії інформації. Для лінійної системи було доведено, що необхідна і достатня умова для максимізації взаємної інформації між станом та оцінкою полягає в мінімізації ентропії оцінки похибки. Також був отриманий фільтр Калмана-Бьюсі для системи як з дискретним, так і неперервним часом шляхом застосування теорії інформації.

У роботі [25] розглянуто проблему оптимального оцінювання стану або фільтрації в стохастичних системах з використанням підходу, що базується на інформаційних мірах. У цьому випадку традиційна мінімальна середньоквадратична міра порівнюється з інформаційними мірами. Переглянуто теорію фільтрації Калмана, для якої запропоновано деякі нові інтерпретації. Було показано, що для лінійної гаусівської системи, фільтр Калмана є оптимальним фільтром не тільки для міри на основі середньоквадратичної похибки, але й для кількох інших інформаційних мір, які були запропоновані в [25].

У роботі [26] отримано рекурсивне рівняння типу Калмана-Б'юсі для оцінки станів. Подібно до цієї роботи ми тут також припускаємо, що необхідно оцінити у найкращому (в певному сенсі) вектор стану $x(T)$ на основі спостережень за функцією $y(t), t = \overline{0, T-1}$. Очевидно, що щоб знайти оцінку компонента вектора $x(T)$, достатньо мати змогу знайти оцінку виразу $a^{\mathrm{T}}x(T)$ для будь-якого вектора $a \in R^n$.

У [27] інформаційний критерій був застосований для оцінки стану лінійних динамічних систем з неперервним часом при наявності випадкових збурень на вході і виході. Проблема пошуку найкращої інформаційної оцінки була зведена до задачі оптимального керування.

Тут ми застосуємо основні ідеї конструктивного методу, які були запропоновані в [26], [27] та [28] для дескрипторної системи (3).

Отже, проблема оцінювання полягає в тому, щоб знайти для (3) оцінку $a^T\hat{x}(T)$ для довільного вектора $a \in R^n$. Таку оцінку ми представляємо у вигляді

$$a^T\hat{x}(T) = \sum_{t=0}^{T-1} \upsilon^T(t)y(t), \tag{4}$$

де $\upsilon(t) \in \mathrm{R}^p$. Наші міркування ґрунтуватимуться на понятті взаємної інформації [29].

Означення 1. Взаємною інформацією між випадковими векторами ξ та η є величина

$$\mathrm{I}(\xi, \eta) = \mathrm{E}\log\frac{p(\xi, \eta)}{p(\xi)p\ \eta)},$$

де $p(\xi\,\eta)$ – функція щільності спільного розподілу ξ та η; $p(\xi)$ та $p(\eta)$ є функціями щільності відособлених розподілів ξ та η відповідно.

Означення 2. Оцінка (4) при $\upsilon(t) = \upsilon^*(t)$ називається інформаційною мінімаксною оцінкою для мережевої моделі (3), якщо

$$\upsilon^*(t) = \arg\sup_{\upsilon(t)}\inf_{n(*)\in G} I(a^Tx(T), \overline{a^Tx(T)}),\ t = \overline{0, T-1},$$
$$\sup\left|E(a^T(T) - \overline{a^Tx(T)})\right| \le C;\ u_x(t) \in G_1(t); \tag{5}$$
$$\overline{a^Tx(T)} = \lambda a^Tx(T \setminus T-1),\ u_y(t) \in G_2(t)$$

для деякої заданої додатньої сталої C.

Твердження 1. Інформаційна мінімаксна оцінка скалярного добутку $a^{\mathrm{T}}x(t)$ на основі спостереження $y(t)$ (3) має вигляд

$$\alpha^Tx(T) = \lambda\alpha^T\hat{x}(T|T-1),$$

де $\hat{x}$ задовольняє рекурентне рівняння

$$\hat{x}(t+1|t) = A(t)\hat{x}(t|t-1) + A(t)K(t)\{y(t) - C(t)\hat{x}(t|t-1)\}\ \hat{x}(0|-1) = Ex(0), \tag{6}$$

де $K(t)$ визначається із співвідношення

$$K(t) = P(t|t-1)C^{\mathrm{T}}\{C(t)P(t|t-1)C^{\mathrm{T}}(t) + Q^{-1}\}^{-1}, \tag{7}$$

де

$$P(t+1|t) = A(t)P(t|t-1)A^{\mathrm{T}}(t) - A(t)P(t|t-1)C^{\mathrm{T}}(t)\{C(t)P(t|t-1)C^{\mathrm{T}}(t) + Q^{-1}\}^{-1} * \tag{8}$$
$$*C(t)P(t|t-1)A^{\mathrm{T}}(t) + R(t),\quad P(0|-1) = R_0.$$

Тут $\lambda \neq 0$ визначається з наступних виразів:

– $\max(0,\lambda_1) < \lambda \le \lambda_2$, якщо $\lambda > 0$;

– $\lambda_1 \le \lambda \le \min(0,\lambda_2)$, якщо $\lambda < 0$, де λ_1, λ_2, корені рівняння;

$$\sum_{t=0}^{T-1}(z_1^T(t)Q_1^{-1}z_1(t))^{1/2} + (z_1(-1), m_0) + \sup_{u_y(t)\in G_2(t)}\left|\sum_{t=0}^{T-1}(u(t), u_y(t))\right| - C = 0, \tag{9}$$

де

$$\hat{\upsilon} = Q(t)C(t)(\lambda p(t) - p_1(t)),\ t = \overline{0, T-1}, \tag{10}$$

де p та p_1 є розв'язками,

$$p(t+1) = A(t)p(t) + R(t)z(t+1),\ p(0) = R_0z(0); \tag{11}$$

$$p_1(t+1) = A(t)p_1(t) + R(t)z_1(t+1),\quad p_1(0) = R_0z_1(0), \tag{12}$$

де вектори $z(t)$ та $z_1(t)$ визначаються за формулами:

$$z_1(t) = A^T(t)z_1(t+1) + C^T(t)v(t),\ z_1(T) = 0; \tag{13}$$

$$z(t) = A^T(t)z(t+1);\ z(T) = a. \tag{14}$$

Зауваження 1. Зазначимо, що надалі можна опустити транспонування матриці $A(t)$ через припущення про симетричність $A(t)$ для моделі мережі (3).

Для обґрунтування такого конструктивного підходу розрахунку інформаційної мінімаксної оцінки використовується наступний результат.

Твердження 2. Оцінка вигляду (4), що визначається критерієм (5), при умові, що модель має вигляд

$$x(t+1) = A(t)x(t) + \varepsilon(t),\quad x(0) = x_0, Ex_0 = 0; \tag{15}$$

$$y(t) = C(t)x(t) + \eta(t) \tag{16}$$

і всі припущення щодо інших змінних мають місце, є незміщеною.

Крім того, задача (4), (5), (15), (16) є тотожньою до задачі оптимального керування для системи (13) та максимізації критерію якості

$$J(\upsilon)=\left[\sum_{t=0}^{T-1} z_1^{\mathrm{T}}(\upsilon,t+1)R(t)z(t+1)+z_1^{\mathrm{T}}(\upsilon,0)R_0 z(0)\right]^2 *$$
$$\left[\sum_{t=0}^{T-1} z^{\mathrm{T}}(t+1)R(t)z(t+1)+z^{\mathrm{T}}(0)R_0 z(0)\right]^{-1} * \quad (17)$$
$$\left[\sum_{k=0}^{T-1} z_1^{\mathrm{T}}(\upsilon,t+1)R(t)z_1(\upsilon,t+1)+\sum_{t=0}^{T-1}\upsilon^{\mathrm{T}}(t)Q^{-1}(t)\upsilon(t)+z_1^{\mathrm{T}}(\upsilon,0)R_0 z_2(\upsilon,0)\right]^{-2},$$

де z є розв'язком системи (14). Тобто задача оцінювання системи без атаки може бути зведена до задачі оптимального керування.

На основі Твердження 2 проблема оцінювання зводиться до задачі оптимального керування. Оптимальне керування $\hat{\upsilon}$ можна знайти, прирівнявши до нуля слабку похідну Гато функціоналу

$$\frac{dJ(\hat{\upsilon}+\in\omega)}{d\in}|_{\in=0}\equiv 0. \quad (18)$$

Відділивши частину, яка є лінійною щодо ω, ми вводимо вектори p і p_1. Таким чином ми можемо отримати оптимальне керування $\hat{\upsilon}$ у вигляді

$$\hat{\upsilon}=Q(t)C(t)(\lambda p(t)-p_1(t)),\quad t=\overline{0,T-1}$$

та отримати оцінку $a^T\hat{x}(T)$.

Умову для λ можна легко отримати, підставивши $a^T x(T)$ та $\overline{a^T x(T)}$ у критерій.

Наслідок 1. Інформаційна мінімаксна оцінка, отримана в Твердженні 1, співпадає з точністю до сталого множника з оптимальною середньоквадратичною оцінкою.

Маємо такий вираз для похибки оцінювання

$$\sup_{\substack{\upsilon(t),\\ t=0,T-1}}\inf_{n(*)\in G} I(a^T x(T),\overline{a^T x(T)})=-\frac{1}{2}\log\left[1-\frac{a^{\mathrm{T}}\hat{p}_1(T)}{a^{\mathrm{T}}p(T)}\right].$$

4. Результати моделювання дескрипторної системи.

Дані для цього прикладу використані з [30]. Модельована система розглядається в дискретному часі на основі моделі у вигляді (2) при

$$A=\begin{pmatrix}0.05 & 1 & 0\\ -0.25 & 0.05 & 0\\ 0.025 & 0.025 & 1\end{pmatrix},\ C=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Система піддається білому гаусівському шумові з нульовим середнім і коваріаційною матрицею $R(t)=R$ вигляду (див. рис. 2):

$$R=\begin{pmatrix}2.53706e-04 & 1.370836e-05 & -0.0001357441\\ 1.370836e-05 & 4.624875e-04 & 0.0002487681\\ -1.357441e-04 & 2.487681e-04 & 0.0002349471\end{pmatrix}.$$

Значення $\eta(t)$ випадковим чином генеруються на основі заданої матриці

$$Q=\sigma^2\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},\ \sigma^2=0.0125.$$

Динаміка системи піддається атаці стану

$$u_x=\begin{Bmatrix}(0.5,0.5,0.5)^{\mathrm{T}}, & якщо & t=7.*i, & i\in N\\ (0,0,0)^{\mathrm{T}}, & інакше & & \end{Bmatrix}.$$

На рисунку 1 представлені результати моделювання дескрипторної системи (2) без білого шуму і без будь-яких атак. На рисунках 3, 4, 5 представлені результати моделювання з урахуванням впливу білого шуму та атаки стану. В результаті застосування Твердження 1 отримано мінімаксну оцінку (рис. 6).

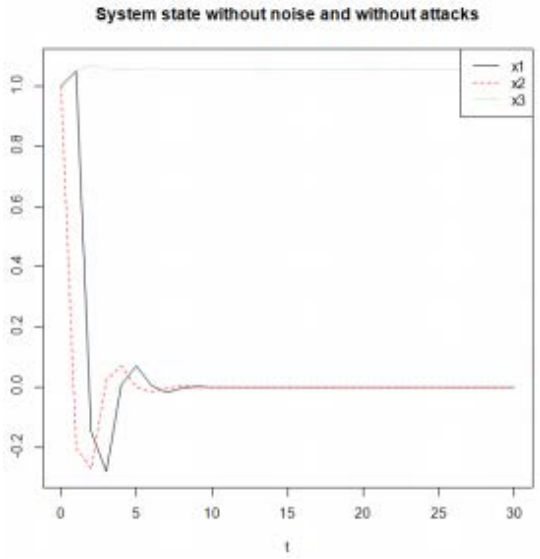

Рис. 1. Стан системи без шуму і без атак

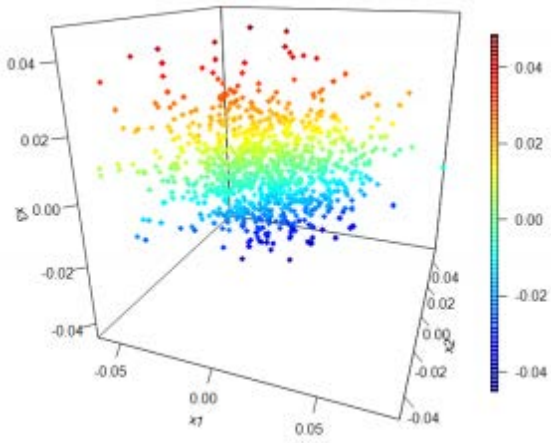

Рис. 2. Білий шум

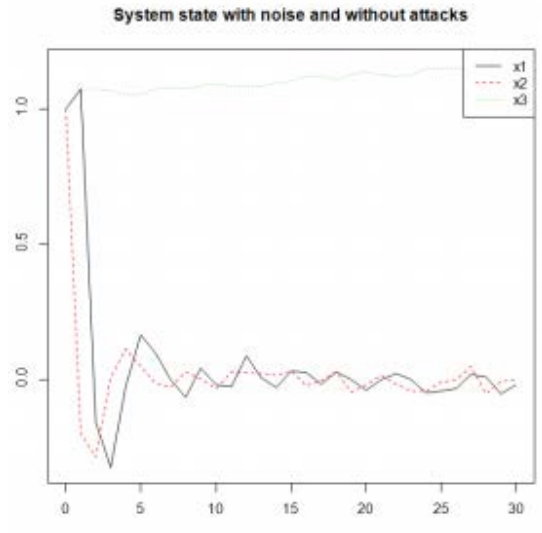

Рис. 3. Стан системи з шумом і без атак

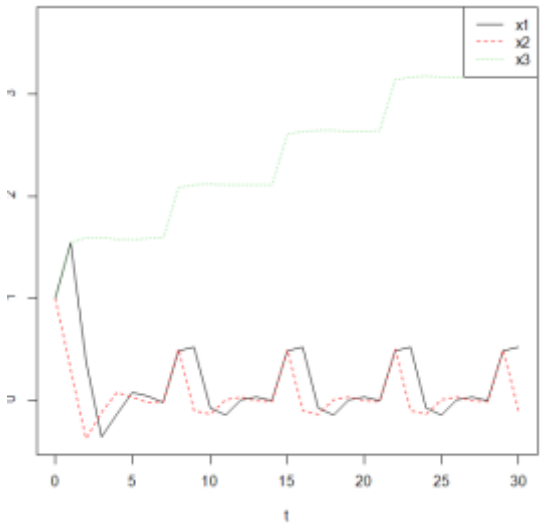

Рис. 4. Стан системи без шуму і з атаками

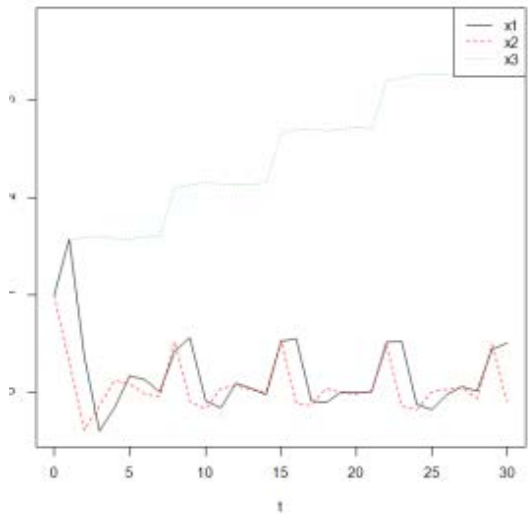

Рис. 5. Стан системи з шумом і атаками

Оцінка x_3 може бути застосована тільки для обмеженого інтервалу часу. Починаючи з $t \approx 20$ похибка збільшується нескінченно. Цей ефект пояснюється постійним впливом атаки стану.

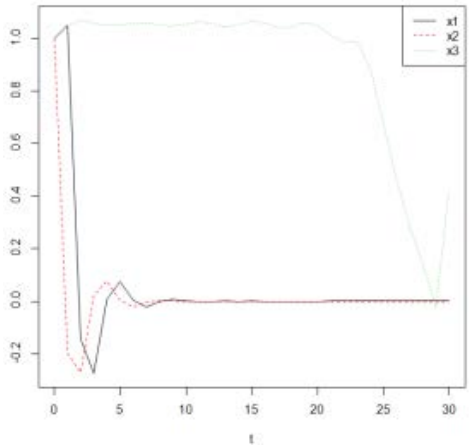

Рис. 6. Оцінка з урахуванням шуму і атак

Висновки

У роботі запропоновано алгоритм побудови оптимальної оцінки для скалярного добутку, що включає стан мережевої моделі під час атаки. Взаємна інформація між випадковими векторами використовувалася як критерій якості для оптимізації.

Оцінювання виконувалося у вигляді скалярного добутку, що включає вектор вимірювань. Розглядаючи ефекти атак на цю оцінку, слід зазначити, що побудована оцінка залежить від таких атак лише через множник λ. Отже, середньоквадратичної похибка такої оцінки не залежить від атаки.

Причиною відсутності впливу атаки на середньоквадратичну похибку є квадратична форма множин, які вибрані для атак стану u_x. Дане припущення дає змогу застосувати апарат лінійно-квадратичної оптимізації, що зводить проблему оцінювання до задачі оптимального керування. На жаль, на практиці ця умова не завжди виконується і тому необхідно розглядати мережі під впливом атак, що належать до складніших множин і, ймовірно, з вектором атаки u, який є випадковим вектором.

ЛІТЕРАТУРА

[1]. E.A Lee, "Cyber physical systems: Design challenges", *11th IEEE international symposium on object oriented real-time distributed computing (isorc)*, pp. 363-369, 2008.

[2]. J. Lee, B. Bagheri, H. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems", *Manufacturing Letters*, vol. 3, pp. 18-23, 2015.

[3]. A. R. Metke and R. L. Ekl, "Security technology for smart grid networks", *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99-107, 2010.

[4]. S. Sridhar, A. Hahn, M. Govindarasu, "Cyber–physical system security for the electric power grid", *Proceedings of the IEEE*, vol. 99, no. 1, pp. 1-15, 2012.

[5]. J. Slay and M. Miller, "Lessons learned from the Maroochy water breach", Critical Infrastructure Protection, vol. 253, pp. 73-82, 2007.

[6]. A. A. Cardenas, S. Amin, S. Sastry, "Research challenges for the security of control systems", *Proceedings of the 3rd Conference on Hot Topics in Security*, Berkeley, CA, USA, 2008, pp. 6:1-6:6.

[7]. S. X. Ding, "Model-Based Fault Diagnosis Techniques: Design Schemes, Algorithms, and Tools", Springer, 2008.

[8]. A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, "Challenges for securing cyber physical systems", *Workshop on Future Directions in Cyber-physical Systems Security, Newark*, NJ, USA, Jul. 2009.

[9]. C. DeMarco, J. Sariashkar, F. Alvarado, "The potential for malicious control in a competitive power systems environment", *IEEE Int. Conf. on Control Applications*, Dearborn, MI, USA, 1996, pp. 462-467.

[10]. S. Amin, A. Cardenas, and S. Sastry, "Safe and secure networked ´ control systems under denial-of-service attacks", Hybrid Systems: Computation and Control, vol. 5469, Apr. 2009, pp. 31-45.

[11]. Y. Liu, M. K. Reiter, P. Ning, "False data injection attacks against state estimation in electric power grids", *ACM Conference on Computer and Communications Security*, Chicago, IL, USA, Nov. 2009, pp. 21-32.

[12]. A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, S. Sastry, "Cyber security analysis of state estimators in electric power systems", I*EEE Conf. on Decision and Control,* Atlanta, GA, USA, Dec. 2010, pp. 5991-5998.

[13]. S. Amin, X. Litrico, S.S. Sastry, A.M. Bayen, "Stealthy deception attacks on water SCADA systems", *Hybrid Systems: Computation and Control*, Stockholm, Sweden, Apr. 2010, pp. 161-170.

[14]. Y. Mo, B. Sinopoli, "Secure control against replay attacks", *Allerton Conf. on Communications, Control and Computing, Monticello*, IL, USA, Sep. 2010, pp. 911-918.

[15]. R. Smith, "A decoupled feedback structure for covertly appropriating network control systems", *IFAC World Congress*, Milan, Italy, Aug. 2011, pp. 90-95.

[16]. M. Zhu, S. Mart´ınez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems", *American Control Conference*, San Francisco, CA, USA, Jul. 2011, pp. 4063-4068.

[17]. F. Hamza, P. Tabuada, S. Diggavi, "Secure state-estimation for dynamical systems under active adversaries", *Allerton Conf. on Communications, Control and Computing*, Sep. 2011.

[18]. G. Dan, H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems", *IEEE Int. Conf. on Smart Grid Communications*, Gaithersburg, MD, USA, Oct. 2010, pp. 214-219.

[19]. E. Levrat, B. Iung, A. Crespo Marquez, "E-maintenance: review and conceptual framework", *Production Planning & Control*, Vol. 19, no. 4, June 2008, pp. 408-429.

[20]. S. Ruiz-Arenas, I. Horváth, R. Mejía-Gutiérrez, E. Opiyo, "Towards the maintenance principles of cyber-physical systems", *Strojniški vestnik-Journal of Mechanical Engineering*, vol. 60 (12), pp. 815-831, 2014.

[21]. F. Pasqualetti, R. Zampieri, and F. Bullo, *Controllability metrics and algorithms for complex networks*, 2013.

[22]. F. Pasqualetti, F. Dorer, and F. Bullo, *Attack detec-tion and identification for cyber-physical systems, Part I: Models and fundamental limitations*.

[23]. L. Rossman, "Epanet 2, water distribution system modeling software", *US Environmental Protection Agency, Water Supply and Water Resources Division*, Tech. Rep., 2000.

[24]. Y. Tomita, S. Omatu, T. Soeda, "An application of the information theory to _ltering problems", *Information Sciences*, vol. 11, no. 1, pp. 13-27, 1976. [Online]. Available: http:// www. sciencedirect. com/ science/ article/pii/0020025576900347.

[25]. X. Feng, K. Loparo, and Y. Fang, "Optimal state estimation for stochastic systems: An information theoretic approach", *Automatic Control, IEEE Transactions*, vol. 42, no. 6, pp. 771-785, Jun. 1997, issn: 0018-9286. doi: 10.1109/9.587329.

[26]. N. Kirichenko, A. Nakonechnyi, "Minimax approach to recursive estimation of states of linear dynamic systems", *Cybernetics*, vol. 13, no. 4, pp. 527-531, 1977, issn: 1573-8337. doi: 10.1007/BF01069547. [Online]. Available: http://dx.doi.org/10.1007/BF01069547.

[27]. A. Nakonechnyi, O. Levoshich, "Estimating the solutions of linear stochastic equations by the information criterion", *Journal of Soviet Mathematics*, vol. 60, no. 4, pp. 1619-1625, 1992, issn: 1573-8795. doi: 10.1007/BF01097620. [Online]. Available: http://dx.doi.org/10.1007/BF01097620.

[28]. A. Nakonechny, V. Marzeniuk, "Uncertainties in medical processes control", *Lecture Notes in Economics and Mathematical Systems*, vol. 581, pp. 185-192, 2006, doi: 10.1007/3-540-35262-7_11. [Online]. Available: https://www.scopus.com/inward/record. uri?eid=2-s2.0-53749093113&partnerID=40&md5=e06a573bf8b6cdcdccd6dc91aecd2626.

[29]. D. MacKay, Information theory, inference, and learning algorithms. Cambridge, UK New York: Cambridge University Press, 2003, isbn: 0521642981.

[30]. R. Waschburger and R. K. H. Galva, "Time delay estimation in discretetime state-space models", Signal Process., vol. 93, no. 4, pp. 904-912, Apr. 2013, issn: 0165-1684. doi: 10.1016/j.sigpro.2012.10.017. [Online]. Available: http:// dx. doi. org/10.1016/j.sigpro.2012. 10.017.

ON MODEL OF CYBER-PHYSICAL SYSTEM WITH STATE AND MEASUREMENT ATTACKS ON THE BASIS OF STOCHASTIC DIFFERENCE EQUATIONS

The article is devoted to questions of simulation of cyber-physical systems taking into account information threats. The principles of organization of structure and reliable functioning of the studied systems are analyzed. The conceptual model of cyber-physical systems taking into account information threats is presented. The constructive algorithm for finding an estimation in a cyberphysical

model during attacks on a state and observation on the basis of measuring system indices is proposed in the work. The model is presented as a non-stationary descriptor system, which includes differential equations for node state variables and algebraic equations for measurements. State variables and measurements are considered as random vectors. The information criterion is used to find the optimal estimate of the scalar product that characterizes the state of the system. The algorithm is based on the construction of the task of estimation to the problem of optimal control. The value of the mean square error that does not depend on attacks is obtained. The evaluation was carried out in the form of a scalar product, which includes a measurement vector. An algorithm for constructing an optimal estimation for a scalar product is proposed, which includes the state of the network model during an attack. Mutual information between random vectors was used as a quality criterion for optimization. The evaluation was carried out in the form of a scalar product, which includes a measurement vector. Considering the effects of attacks on this estimate, it should be noted that the build estimate depends on such attacks only through the multiplier. The average square error of such an estimate is independent of the attack. The reason for the absence of impact of the attack on the mean square error is the quadratic form of the sets that are selected for state attacks. This assumption makes it possible to apply a linear-quadratic optimization device, which reduces the problem of evaluation to the problem of optimal control. Received results illustrated in the numerical example for the stage of system without noise and with attacks and for the stage of system with noise and attacks. In this case , a three-node cyberphysical system was used which could be used for planning technical service and optimized management for achievement more high totalperformance and safety of the studied systems .
Keywords: cyber-physical system, stochastic difference equations, optimal estimation problem, network model.

О МОДЕЛИ КИБЕР-ФИЗИЧЕСКОЙ СИСТЕМЫ С АТАКОЙ СОСТОЯНИЯ И ИЗМЕРЕНИЙ НА ОСНОВЕ СТОХАСТИЧЕСКИХ РАЗНОСТНЫХ УРАВНЕНИЙ

Статья посвящена вопросам моделирования киберфизических систем с учетом информационных угроз. Проанализированы принципы организации структуры и надежного функционирования исследуемых систем. Приведена концептуальная модель кибер-физических систем на базе информационных угроз. В работе предложено конструктивный алгоритм для поиска оценки в киберфизичний модели при атаках на состояние и наблюдения на основе измерения показателей системы. Модель представлена в виде нестационарной дескрипторной системы, которая включает дифференциальные уравнения для переменных состояния узла и алгебраические уравнения для измерений. Переменные состояния и измерения считаются случайными векторами. Использованный информационный критерий, с целью нахождения оптимальной оценки скалярного произведения, каторая характеризует состояние системы. Алгоритм основывается на сведении задачи оценивания к задаче оптимального управления. Получено значение среднеквадратической погрешности, каторая не зависит от атак. Оценивания выполнялось в виде скалярного произведения, включая вектор измерений. Предложен алгоритм построения оптимальной оценки для скалярного произведения, включая состояние сетевой модели во время атаки. Взаимная информация между случайными векторами использовалась как критерий качества для оптимизации. Оценивание выполнялось в виде скалярного произведения, включая вектор измерений. Рассматривая эффекты атак на эту оценку, сделано вывод, что построена оценка зависит от таких атак только через множитель. Среднеквадратическая погрешность такой оценки не зависит от атаки. Причиной отсутствия влияния атаки на среднеквадратическую погрешность есть квадратическая форма множеств, которые выбраны для атак состояния. Данное предположение позволяет применить аппарат линейно-квадратичной оптимизации, каторый сводит проблему оценки к задаче оптимального управления. Полученные результаты проиллюстрировано на численном примере для состояния системы без шума и с атаками и состояния системы с шумом и атаками. При этом было использовано трьохузловую киберфизическую систему, которая может использоваться для планирования технического обслуживания и оптимизированного управления для достижения более высокой общей производительности и безопасности исследуемых систем.
Ключевые слова: кибер-физическая система, стохастические разностные уравнения, задача оптимального оценивания, сетевая модель.

Марценюк Василь Петрович, доктор технічних наук, професор, професор кафедри інформатики та автоматики Університету в Бельско-Бялій.
E-mail: vmartsenyuk@ath.bielsko.pl.
Orcid ID: 0000-0001-5622-1038.
Марценюк Василий Петрович, доктор технических наук, профессор, профессор кафедры информатики и автоматики, Университета в Бельско-Бялой.
Martsenyuk Vasyl, Doctor of Technical Sciences, Professor, Professor of the Department of Informatics and Automatics, University of Bielsko-Biala, Bielsko-Biala.

Сверстюк Андрій Степанович, кандидат технічних наук, доцент, доцент кафедри медичної інформатики, Тернопільского державного медичного університету імені І. Я. Горбачевського.
E-mail: sverstyuk@tdmu.edu.ua.
Orcid ID: 0000-0001-8644-0776.
Сверстюк Андрей Степанович, кандидат технических наук, доцент, доцент кафедры медицинской информатики, Тернопольского государственного медицинского университета имени И. Я. Горбачевского.
Sverstiuk Andriy, PhD, Associate Professor of Technical Sciences, Associate Professor, Associate Professor, Department of Medical Informatics, I.Y. Gorbachevsky Ternopil State Medical University.