DOI: 10.20535/kpisn.2025.1.322905
УДК 004.056:519.8

О.М. Новіков[1*], М.І. Ільїн[1], І.В. Стьопочкіна[1], М.В. Овчарук[1]
[1]Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
*Відповідальний автор: o.novikov@kpi.ua

ВИЗНАЧЕННЯ ПАРАМЕТРІВ НЕПОМІТНИХ КІБЕРАТАК НА СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Проблематика. Інтеграція систем промислового контролю із сучасними мережевими технологіями спричиняє виникнення великої кількості атак на критичну інфраструктуру. Методи виявлення і протидії таким атакам ще недостатньо розвинені, є нагальна потреба у розвитку математичного апарату, який дозволяє визначати параметри кібератак на такі системи.
Мета дослідження. Метою роботи є розроблення й дослідження параметрів непомітної атаки (Stealthy attack) на систему керування об'єкта критичної інфраструктури як інструменту тестування систем кіберзахисту, яка обходить стандартний детектор діагностики несправностей.
Методика реалізації. Модель системи промислового контролю розглянуто у вигляді диференціального рівняння. Введено параметри адитивної атаки на керування, а також критерій детектування несправностей. Задачу визначення параметрів розв'язано методами оптимального керування з використанням функціонала Лагранжа та методу градієнтного спуску.
Результати дослідження. Запропоновано новий метод і відповідний алгоритм пошуку шкідливих спотворень керування з використанням варіаційного методу оптимізації та градієнтного методу найшвидшого спуску. Проведено обчислювальний експеримент, який свідчить про працездатність запропонованого алгоритму.
Висновки. Розглянуто кібератаку із класу непомітних атак (Stealthy attacks), спрямовану на модифікацію керуючих сигналів системи керування об'єктами критичної інфраструктури, яка здатна обходити стандартні детектори несправностей. Запропоновані метод та алгоритм можуть бути застосовані під час планування тестів на проникнення для аналізу безпеки автоматизованих систем контролю об'єктів критичної інфраструктури індустріального типу. Працездатність алгоритму перевірено комп'ютерним експериментом.
Ключові слова: теорія керування; кібербезпека; непомітні атаки; визначення параметрів.

Вступ

Останнім часом відбулося значне зростання інтенсивності кібератак на об'єкти критичної інфраструктури, і це загрозливе явище обумовлено насамперед вразливостями, притаманними сучасним автоматизованим системам управління технологічними процесами ((АСУ ТП), чи англ. Industrial Control System (ICS)), системам диспетчерського управління та збору даних (SCADA – Supervisory Control and Data Acquisition), розподіленим системам керування (DCS – Distributed Control System), системам програмованих логічних контролерів (PLC – Programmable Logic Controller).

Сучасні автоматизовані системи все частіше інтегруються в інформаційні мережі, щоб забезпечити гнучкість, продуктивність і віддалений доступ. Утім, ця інтеграція часто відбувається у формі формального кількісного об'єднання підсистем без аналізу умов їх безпечної взаємодії, що створює серйозні загрози безпеки функціювання новостворених систем. Серед таких загроз можна назвати застарілі протоколи окремих підсистем, відсутність шифрування, розширення доступу з боку мереж загального доступу, інтеграцію з Інтернетом речей (IoT). Хоча нині активно впроваджуються сучасні технології, багато використовуваних систем розроблялися десятиліття тому – у них використовуються

Пропозиція для цитування цієї статті: О.М. Новіков, М.І. Ільїн, І.В. Стьопочкіна, М.В. Овчарук, "Визначення параметрів непомітних кібератак на системи керування об'єктів критичної інфраструктури", *Наукові вісті КПІ*, № 1, с. 69–75, 2024. doi: 10.20535/kpisn.2025.1.322905

Offer a citation for this article: Oleksii Novikov, Mykola Ilin, Iryna Stopochkina, Mykola Ovcharuk, "Determination of parameters of stealthy cyber attacks on control systems of critical infrastructure objects", *KPI Science News*, no. 1, pp. 69–75, 2025. doi: 10.20535/kpisn.2025.1.322905

застарілі протоколи, не враховуються сучасні кіберзагрози. Безпека лише за рахунок організаційних факторів, фізичної ізоляції в сучасних умовах перестає бути достатньою. Типовими випадками є використання незахищених протоколів передачі даних, які роблять можливими атаки типу «людина посередині», загрози перехоплення, повтор і фальсифікації даних, які передаються. Під час підключень таких систем до Інтернету та їх інтеграції із пристроями IoT для виконання завдань моніторингу й управління на хмарному рівні неминуче розширюється поверхня атак і вразливі механізми стають ціллю кібератак зловмисників.

У сучасних умовах кіберпростір став середовищем для реалізації різноманітних цілей, зокрема впровадження шкідливих впливів унаслідок політичних мотивів, реалізації економічного протиборства, екологічного хактивізму, тероризму та інших цілей кіберзлочинців. Таким чином, кібератаки роблять можливими ведення гібридної війни, зменшення економічного потенціалу країни або терористичних дій. У відомих прикладах кібератак на об'єкти енергетики використовувались прийоми соціальної інженерії разом зі шкідливими програмами-вимагачами (ransomware), деякі установи секторів критичної інфраструктури потерпають від викрадення комерційних таємниць тощо.

Сектори критичної інфраструктури охоплюють майже всі сфери людської діяльності – починаючи з індустрії і завершуючи службами охорони здоров'я. Унаслідок цифровізації суспільства відбувається перехід на роботу з електронними даними, комп'ютеризацію всіх видів діяльності. Серед секторів критичної інфраструктури – енергетика, водопостачання, транспорт, фінансова сфера, хімічна промисловість і важка індустрія, охорона здоров'я, комунікації та інші. Разом зі збільшенням масштабів і взаємозалежностей між різними підприємствами, зростанням складності задіяних у них систем контролю, відкритістю до зовнішніх мереж зростає і кількість кібератак.

Оскільки одним із критеріїв віднесення об'єкта до критичної інфраструктури є його потенціальний вплив на людське суспільство, тяжкість наслідків, спричинених припиненням нормального функціонування такого об'єкта, можна стверджувати, що потенціальна шкідливість успішних атак для таких об'єктів є високою й істотною для міст, регіонів або ж усієї країни залежно від рівня критичності такого об'єкта. Унаслідок глобалізації економіки різних країн є суттєво взаємозалежними, тому успішні атаки на об'єкти критичної інфраструктури є джерелом значних фінансових втрат і порушенням функціонування цілих секторів або дестабілізації економіки цілих країн чи регіонів.

Інтенсивність кібератак на об'єкти критичної інфраструктури зросла через поєднання технологічних, економічних і політичних факторів. Зловмисники використовують слабкі місця ICS, SCADA, DCS та PLC для досягнення своїх цілей, що робить завдання забезпечення кіберзахисту критично важливим. Це вимагає від держав та організацій розробляти більш складні системи захисту та постійно вдосконалювати наявні інструменти кібербезпеки.

Захист систем нижнього рівня, зокрема PLC, є ключовим елементом у забезпеченні кібербезпеки критичної інфраструктури. Вразливість PLC робить їх основними цілями атак, наслідки яких можуть бути катастрофічними. Розвиток сучасних систем виявлення атак та адаптивних механізмів захисту має бути пріоритетом для промисловості й держав.

Системи автоматизованого управління технологічними процесами нижнього рівня, які ґрунтуються на PLC, є найбільш вразливими до атак і водночас критично важливими з точки зору наслідків їх ураження. Ці системи відіграють ключову роль у підтриманні основних технологічних параметрів у критичних галузях.

Серед найпоширеніших атак на системи автоматизації нижнього рівня або безпосередньо на програмовані логічні контролери PLC можна виділити атаки відмови в обслуговуванні (DoS attacks), які мають за мету паралізувати роботу PLC через перевантаження комунікаційного каналу або процесора, атаки повторного використання даних (Replay attacks), які повторюють раніше захоплені сигнали, змушуючи PLC виконувати небажані дії, маніпуляції через впровадження фальшивих даних (False data injection attacks), які вводять хибні дані до системи для введення оператора чи алгоритмів в оману. Відомими також є декілька схожих атак: атаки з нульовою динамікою (Zero dynamic attacks), які маніпулюють сигналами так, щоб зміни не впливали на видимі стани системи, приховані атаки (Covert attacks), які залишаються непомітними для системи моніторингу, непомітні атаки (Stealthy attacks), які впроваджують зміни, що не викликають сигналів тривоги у системах моніторингу [1–6].

Рівень загрози таких атак значною мірою залежить від наявності сучасних систем виявлення кібератак у промислових автоматизованих

системах. Нині доступний широкий спектр методів і систем для виявлення атак, які постійно вдосконалюються. Вони варіюються від традиційних підходів діагностики несправностей у програмному забезпеченні до сучасних методів, що ґрунтуються на аналізі поведінкових характеристик, штучному інтелекті, методах обробки даних, що здатні підтримувати швидке реагування на аномалії.

У низці досліджень [7–11] було проаналізовано традиційні підходи до діагностики несправностей, такі як байєсове виявлення з бінарною гіпотезою (Bayesian detection with binary hypothesis), метод зважених найменших квадратів (Weighted least squares), χ^2-детектори на основі фільтрів Калмана (χ^2-detector based on Kalman filters), а також техніки виявлення та ізоляції несправностей (Fault Detection and Isolation techniques).

Розвиток методів виявлення атак сприяє підвищенню рівня кіберзахисту. Водночас посилюється потреба вивчати нові та вже відомі кібератаки, які можна використовувати як інструмент для тестування ефективності систем захисту. Зокрема, значний інтерес для наукових досліджень становлять атаки з нульовою динамікою (Zero dynamic attacks), приховані атаки (Covert attacks), непомітні атаки (Stealthy attacks) та інші види, здатні обходити традиційні детектори діагностики.

Постановка задачі

Метою роботи є розроблення і дослідження параметрів непомітної атаки (Stealthy attack) на систему керування об'єкта критичної інфраструктури як інструмента тестування систем кіберзахисту, яка обходить стандартний детектор діагностики несправностей.

Модель атаки на систему керування

Розглянемо модель динамічної системи:

$$\frac{dx(t)}{dt} = Ax(t) + Bu(t), \tag{1}$$

$$x(t_0) = x_0, \tag{2}$$

$$y(t) = Cx(t), \tag{3}$$

де $x(t)$ – n-вимірний вектор стану фізичної системи; $y(t)$ – l-вимірний вектор вимірювань датчиків вимірювальної системи; A, B та C – відомі матриці коефіцієнтів відповідної розмірності; $u(t)$ – k-вимірний вектор керування процесом. Співвідношення (1), (2) є моделлю системи, а (3) – модель вимірювальної системи.

Розглянемо задачу оптимального керування станом $x(t)$ лінійної системи (1), (2) за законом керування із зворотним від'ємним зв'язком і квадратичним критерієм якості [12–14]:

$$J = \int_{t_0}^{t_k} \left[x^T(t)Qx(t) + u^T(t)Ru(t) \right] dt, \tag{4}$$

де Q та R – відомі вагові матриці.

Кінцеві співвідношення оптимального керування системою (1), (2) мають вигляд [14]

$$u(t) = -K(t)x(t), \quad K(t) = R^{-1}B^T P(t), \tag{5}$$

де матриця $P(t)$ є рішенням нелінійного рівняння Ріккаті:

$$\frac{dP(t)}{dt} = -P(t)A^T - AP(t) + P(t)BR^{-1}(t)B^T P(t) - Q, \tag{6}$$

$$P(t_k) = P_k. \tag{7}$$

Задачі оптимального керування добре проєктуються на проблеми ICS, SCADA, DCS та PLC об'єктів критичної інфраструктури.

Розглянемо кібератаку, спрямовану на автоматичну систему оптимального керування об'єктом критичної інфраструктури (1), (2), (5), (6). Основною метою такої атаки є порушення нормального функціонування системи через спотворення сигналу керування, який є ключовим елементом у процесі прийняття рішень та управління. У цьому аналізі розглянемо сценарій, де зловмисник здатний лише адитивно модифікувати компоненти сигналу керування (рис. 1).

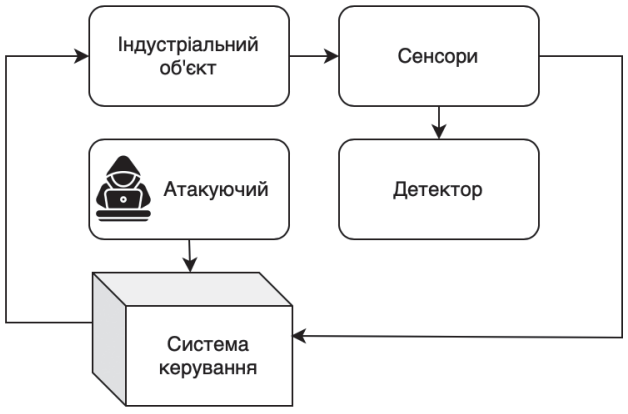

Рис. 1. Атака на керування автоматизованої системи керування

Особливістю досліджуваного випадку є наявність у системі детектора несправностей, який має функцію виявлення аномалій чи втручань у роботу системи. Утім, умовою успішної атаки є її непомітність для цього детектора. Інакше кажучи, зловмисник здійснює атаку класу «непомітних атак» (Stealthy attacks), які спеціально розроблені для уникнення виявлення.

Таким чином, реалізація подібної кібератаки спрямована на порушення цілісності інформації, яка циркулює та обробляється у системі. Це створює загрозу для стабільності й безпеки об'єкта критичної інфраструктури, адже порушення інформаційних процесів може призвести до некоректного функціонування всього комплексу автоматизованого керування.

Для реалізації атаки зловмисник ретельно аналізує систему захисту інформації, що включає збирання даних про архітектуру і структуру автоматичної системи керування, вивчення принципів її роботи, а також отримання доступу до ключових елементів, таких як програмні коди, логіка алгоритмів керування PLC та детектор несправностей. Особливу увагу зловмисник приділяє вивченню методів виявлення несправностей, застосовуваних у системі, щоб обійти їх або залишатися непомітним.

Сформульоване вище дозволяє визначити модель атаки на автоматизовану систему оптимального керування у такому вигляді:

$$a(t) = \left[\tilde{u}(t)\right] = h\left(F, u(t)\right), \qquad (8)$$

де $a(t)$ – вектор атаки; $\tilde{u}(t)$ – спотворене керування, яке перебуває під впливом шкідливих даних; F – показник знань атакуючого щодо об'єкта атаки. Модель керування, яке атаковано, можна записати таким співвідношенням:

$$\tilde{u}(t) = u(t) + u_a(t), \qquad (9)$$

де $u_a(t) \in U_{доп}$ – параметр непомітної атаки (Stealthy attacks), шкідливі дані, додані до керування системи.

Як було зазначено вище, автоматична система оптимального керування оснащена детектором несправностей (рис. 1), розробленим із застосуванням методу зважених найменших квадратів (Weighted Least Squares) [7–11]:

$$J = \int_{t_0}^{t_k} \left[Cx(t) - y(t)\right]^T S^{-1} \left[Cx(t) - y(t)\right] dt, \qquad (10)$$

де $y(t)$ – вимірювання процесу, здійснюване детектором несправностей; S – відомий ваговий коефіцієнт.

Такий метод детектування забезпечує точне оцінювання параметрів і високий рівень чутливості до аномалій у роботі системи. Утім, зловмисник може використати знання про цей метод для формування атак, які мінімізують ризик виявлення. У такій ситуації безпека системи залежить від ступеня захищеності її архітектури, надійності алгоритмів ідентифікації несправностей, а також від здатності швидко адаптуватися до потенційних загроз.

Пошук шкідливого впливу $u_a(t)$ непомітної атаки (Stealthy attacks), що мінімізують показник детектора несправностей $J(u_a)$

Перепишемо співвідношення детектора несправностей (5) у вигляді

$$J(u_a) = \int_{t_0}^{t_k} \left[C\tilde{x}(t) - y(t)\right]^T S^{-1} \left[C\tilde{x}(t) - y(t)\right] dt \to \min_{u_a \in U_{доп}}, \qquad (11)$$

де $\tilde{x}(t)$ – спотворений стан, який перебуває під впливом шкідливого керування u_a, доданого до керування системи $u(t)$. При цьому лінійну систему (1), (5), яка перебуває під впливом кібератаки (6), (7), (9), запишемо таким чином:

$$\frac{d\tilde{x}(t)}{dt} = A\tilde{x}(t) + B\left[-K(t)\tilde{x}(t) + u_a(t)\right], \qquad (12)$$

$$\tilde{x}(0) = \tilde{x}_0, \qquad (13)$$

де $K(t)$ визначають співвідношенням (5).

Таким чином, маємо задачу пошуку шкідливого керування $u_a(t) \in U_{доп}$ непомітної атаки (Stealthy attacks) на систему (12), (13), яке мінімізує значення й обходить детектор діагностики несправностей (11).

Розв'яжемо задачу пошуку екстремуму функціонала (11) з обмеженнями (12), (13) методом Лагранжа [14]. Щоб врахувати обмеження, використаємо множник Лагранжа $\lambda(t)$, який є вектором того ж розміру, що й $\tilde{x}(t)$, а обмеження на $u_a(t) \in U_{доп}$ врахуємо на завершальній стадії алгоритму.

Сформуємо допоміжний функціонал Лагранжа:

$$L\left(\tilde{x}(t), u_a, \lambda\right) = \int_{t_0}^{t_k} \left\{\left[C\tilde{x}(t) - y(t)\right]^T S^{-1} \left[C\tilde{x}(t) - y(t)\right] + \right.$$
$$\left. + \lambda^T(t)\left[A\tilde{x}(t) - B\left[-K(t)\tilde{x}(t) + u_a(t)\right] - \frac{d\tilde{x}(t)}{dt}\right]\right\} dt. \qquad (14)$$

Виходячи з варіаційного принципу, за умови $\partial L / \partial \tilde{x} = 0$, отримаємо спряжене рівняння:

$$\frac{d\lambda(t)}{dt} = -(A^T - K^T B^T)\lambda(t) - \\ -2C^T S^{-1}\left[C\tilde{x}(t) - y(t)\right], \quad (15)$$

$$\lambda(t_k) = 0. \quad (16)$$

Необхідні умови оптимальності відносно невідомого параметра $u_a(t) \in U_{доп}$ мають вигляд

$$\delta L(u_a)\frac{dL}{du_a} = \delta u_a = 0 \forall u_a(t) \in U_{доп}. \quad (17)$$

Умову (17) для $u_a \notin U_{доп}$ доповнимо:

$$\frac{dL}{du_a} = 0 \forall u_a(t) \in U_{доп}. \quad (18)$$

Варіюючи функціонал (14), можна показати, що

$$\frac{dL}{du_a} = \int_{t_0}^{t_k} K^T \lambda(t). \quad (19)$$

Шкідливе керування $u_a(t)$, яке мінімізує показник детектора несправностей $J(u_a)$, будемо шукати з використанням градієнтного методу найшвидшого спуску:

$$u_a^{i+1} = Pr\left\{u_a^i - \alpha\frac{dL^i}{du_a}\right\}, \quad (20)$$

де $Pr\{\cdot\}$ – проєкція рішення $u_a^{i+1}(t)$ на область $u_a(t) \in U_{доп}$; i – номер, а α – відомий крок градієнтного циклу; u_a^0 також відомо.

Пошук невідомої змінної u_a на основі градієнтної процедури (20) закінчується за умови виконання критерію

$$\left|J^i - J^{i+1}\right| / J^i \le \varepsilon, \quad (21)$$

де ε – відома похибка.

Алгоритм пошуку шкідливого керування, що мінімізує показник детектора несправностей

Об'єднуючи співвідношення (12), (13), (15)–(16) із (17)–(21), сформулюємо алгоритм пошуку шкідливого керування u_a, що мінімізує показник детектора несправностей $J(u_a)$:

1. Для $i = 0$, де i – номер кроку градієнтного циклу, надаємо стартове значення u_a^0 та значення кроку градієнтної процедури α.

2. Для кроку $i+1$ за співвідношеннями (17)–(19) розраховуємо dL^i / du_a, де множник Лагранжа $\lambda(t)$ та спотворена оцінка стану $\tilde{x}(t)$, яка перебуває під впливом шкідливого керування u_a, визначені, відповідно, співвідношеннями (15), (16) та (12), (13).

3. Використовуючи (20), визначаємо $u_a^{i+1}(t)$.

4. Розраховуємо (11) і перевіряємо (21). Якщо умова виконується, то завершуємо алгоритм, інакше переходимо до п. 2.

З метою аналізу працездатності розроблених методу та алгоритму визначення параметрів кібератаки на автоматизовану систему об'єкта критичної інфраструктури розглянемо приклад.

Аналіз результатів обчислювального експерименту

Наведемо результати обчислювального експерименту з дослідження розроблених вище методу та алгоритму. Розглянемо технічну систему, яку описують співвідношеннями (1), (2). Треба розв'язати задачу пошуку параметрів непомітної атаки (Stealthy attacks) на систему керування, яка обходить стандартний детектор діагностики несправностей. Для розв'язання задачі використано алгоритм, наведений вище, співвідношення (8)–(21) та вихідні дані, наведені у табл. 1.

Функція Ріккаті, а також вектор-стовпець вимірювань $y(t)$ розраховано окремо, поза градієнтною процедурою пошуку.

Результати експерименту показано на рис. 2 та 3. На рис. 2 подано критерій якості $J(u_a)$, який зменшується і з кожним кроком процедури наближається до нуля. Поведінку шкідливих даних, доданих до керування u_a під час градієнтної процедури, які зловмисник визначає і вводить так, щоб мінімізувати критерій детектора та зробити його дії непомітними для системи моніторингу, зображено на рис. 3.

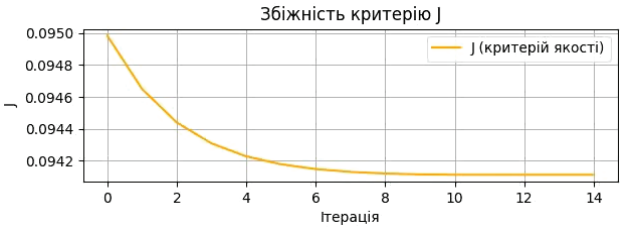

Рис. 2. Збіжність критерію J у процесі ітераційної процедури

Аналізуючи результати обчислювального експерименту можна побачити, що ітераційна градієнтна процедура пошуку шкідливих даних,

***Таблиця* 1.** Вихідні дані обчислювального експерименту пошуку параметрів кібератаки на систему керування

Параметр	Позначення	Значення
Розмірність матриць	A, C, K, P, Q, R, S	2x2
Розмірність векторів-стовпців	$x(t)$, $\tilde{x}(t)$ $\lambda(t)$, $y(t)$, $u_a(t)$	2x1
Матриця коефіцієнтів моделі	A	0; 1; –6; –5
Матриця керування	B	0; 1; 0; 0
Матриця вимірювань	C	1; 0; 0; 1
Вагові матриці критерію системи оптимального керування	Q R	1; 0; 0; 1 1; 0; 0; 1
Вагова матриця фільтра й детектора несправностей	S	1; 0; 0; 1
Початкові умови моделі	$x(0)$	0; 1
Кінцеві умови спряженого рівняння	$\lambda(t_k)$	0; 0
Період дослідження і крок дискретизації у часі	t_0,t_k, Δt	0; 6; 0,01
Розмір і кількість кроків градієнтної процедури	α, N	15,0; 15
Стартове значення параметра пошуку	u_a^0	20,0
Мінімальне допустиме значення шкідливого керування	$u_{a\,\min}$	19,5

доданих до керування збігається до рішення u_a. Останнє надає можливість робити висновок про працездатність запропонованого методу та алгоритму.

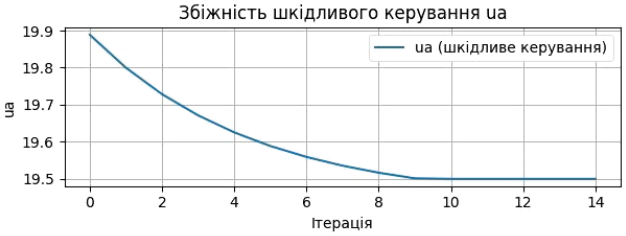

Рис. 3. Збіжність спотворених даних керування u_a

Висновки

Розглянуто кібератаку із класу непомітних атак (Stealthy attacks), спрямовану на модифікацію керуючих сигналів системи керування об'єктами критичної інфраструктури, яка здатна обходити стандартні детектори несправностей. Запропоновано новий метод і відповідний алгоритм пошуку шкідливих спотворень керування з використанням варіаційного методу оптимізації та градієнтного методу найшвидшого спуску.

Проведено обчислювальний експеримент, отримано й проаналізовано кількісні характеристики алгоритму. Аналіз результатів підтвердив працездатність розроблених методу та алгоритму.

Отримані у роботі розв'язки можуть бути застосовані під час планування тестів на проникнення для аналізу безпеки автоматизованих систем контролю об'єктів критичної інфраструктури індустріального типу.

Перспективою наступних досліджень є поширення підходу на основі варіаційних методів оптимізації на інші класи атак, зокрема на атаки, пов'язані із введенням затримок, що належать до класу «відмова в обслуговуванні».

References

[1] Y. Hu *et al.*, "Detecting stealthy attacks against industrial control systems based on residual skewness analysis", *EURASIP Journal on Wireless Communications and Networking*, 2019, no. 74, pp. 1–14. DOI: 10.1186/s13638-019-1389-1

[2] Y. Wang *et al.*, "Cyber-physical systems in industrial process control", *ACM Sigbed Review*, 2008, vol. 5, no. 1, pp. 1–2. DOI: 10.1145/1366283.1366295

[3] A.M. Mohan *et al.*, "A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems", *MDPI Energies*, 2020, vol. 13, no. 3860, pp. 1–33. https://www.mdpi.com/1996-1073/13/15/3860

[4] H.S. Sánchez *et al.*, "Bibliographical review on cyber attacks from a control oriented perspective", *Annual Reviews in Control*, 2019, vol. 48, pp. 103–128. DOI: 10.1016/j.arcontrol.2019.08.002

[5] O. Novikov *et al.*, "Cyber Attacks Simulation for Modern Energy Facilities", *CEUR Workshop Proceedings. Selected Papers of the XXIII International Scientific and Practical Conference "Information Technologies and Security"*, 2023, vol. 3887, pp. 35–49. https://ceur-ws.org/Vol-3887/

[6] L. Alekseichuk *et al.*, "Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry", *Theoretical and Applied Cybersecurity*, 2023, vol. 5, no. 1, pp. 61–66. DOI: 10.20535/tacs.2664-29132023.1.287365

[7] M. Syfert *et al.*, "Integrated Approach to Diagnostics of Failures and Cyber-Attacks in Industrial Control Systems", *MDPI Energies*, 2022, vol. 15, no. 17, pp. 1–24. DOI: 10.3390/en15176212

[8] A.A. Cardenas *et al.*, "Challenges for Securing Cyber Physical Systems", *DHS*, 23 лип. 2009. https://ptolemy.berkeley.edu/projects/chess/pubs/601.html

[9] Y. Mo and B. Sinopoli, "Secure Control Against Replay Attacks", *47th Annual Allerton Conference on Communication, Control, and Computing*, 2009, 30 верес. – 2 жовт. *IEEE Xplore*, pp. 911–918. DOI: 10.1109/Allerton16076.2009

[10] A. Cooper *et al.*, "Anomaly Detection in Power System State Estimation: Review and New Directions", *MDPI Energies*, 2023, vol. 16, no. 18, pp. 1–15. https://www.mdpi.com/1996-1073/16/18/6678

[11] A. Sztyber-Betley *et al.*, "Controller Cyber-Attack Detection and Isolation", *MDPI Sensors*, 2023, vol. 23, no. 5, pp. 1–27. DOI: 10.3390/s23052778

[12] D.E. Kirk *et al.*, "Optimal Control Theory", An Introduction, Mineola, New York: Dover Publications, Inc., 2004, 443 с. https://books.google.com.ua/books?id=fCh2SAtWIdwC&printsec=copyright&redir_esc=y#v=onepage&q&f=false

[13] Ray W. Harmon, "Advanced Process Control", New York: McGraw-Hill Book Company, 1981, 376 с. https://books.google.com.ua/books/about/Advanced_Process_Control.html?id=-7tTAAAAMAAJ&redir_esc=y

[14] A.P. Sage and C.C. White, III. "Optimum Systems Control", New Jersey: Premtice-Hall, 1977, 413 с. https://www.semanticscholar.org/paper/Optimum-systems-control%3A-by-A.-P.-Sage-and-C.-C.-Eslami/83d44a3e6cd41f834a99209a671a248dfef12634#citing-papers

Oleksii Novikov, Mykola Ilin, Iryna Stopochkina, Mykola Ovcharuk

DETERMINATION OF PARAMETERS OF STEALTHY CYBER ATTACKS ON CONTROL SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

Background. Integrating industrial control systems with modern network technologies has significantly increased cyber attacks targeting critical infrastructure. Detection and mitigation methods for such attacks remain underdeveloped, necessitating the advancement of mathematical frameworks capable of identifying attack parameters in such systems.

Objective. The purpose of the paper is to develop and investigate the parameters of a stealthy attack on a critical infrastructure control system. The attack serves as a testing tool for cybersecurity systems by evading standard fault detection mechanisms.

Methods. The industrial control system model is represented as a differential equation. Parameters of an additive attack on the control system are introduced. A fault detection criterion is defined. The problem of determining attack parameters is addressed using optimal state control methods, employing the Lagrange functional and the gradient descent method.

Results. A new method and corresponding algorithm for identifying malicious control distortions using variational optimization and the fast gradient descent method are proposed. A computational experiment confirms the effectiveness of the proposed algorithm.

Conclusions. The paper examines a stealthy attack capable of bypassing standard fault detectors aimed at modifying control signals in critical infrastructure management systems. The proposed method and algorithm can be utilized in penetration testing to assess the security of automated control systems in industrial critical infrastructure. The algorithm's functionality has been validated through computational experiments.

Keywords: control theory; cybersecurity; stealthy attacks; parameter identification.

Рекомендована Радою
Навчально-наукового фізико-технічного інституту
КПІ ім. Ігоря Сікорського

Надійшла до редакції
30 грудня 2024 року

Прийнята до публікації
10 лютого 2025 року