КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1152
УДК 004.056:004.94:004.75

Савченко Тетяна Віталіївна
Кандидат технічних наук, доцент, доцент кафедри інформатики
Національний університет «Києво-Могилянська академія», Київ, Україна
ORCID: 0000-0002-8884-5360
tsavchenko@ukma.edu.ua

Лапіна Софія Олександрівна
Студентка спеціальності «Кібербезпека та захист інформації»
Національний університет «Києво-Могилянська академія», Київ, Україна
ORCID: 0009-0006-5425-9984
s.lapina@ukma.edu.ua

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЦИФРОВИХ ДВІЙНИКІВ У КІБЕРФІЗИЧНИХ СИСТЕМАХ INDUSTRY 4.0

Анотація. У статті представлено комплексний підхід до аналізу, проєктування та практичної реалізації захисту цифрових двійників у кіберфізичних системах Industry 4.0. Актуальність дослідження зумовлена тим, що цифровий двійник у сучасному промисловому середовищі виступає не лише інструментом моніторингу й аналітики, а функціональним компонентом цифрового контуру, компрометація якого здатна спричинити порушення цілісності та достовірності телеметрії, втрату синхронізації між фізичним і цифровим станами, деградацію сервісів і небезпечний вплив на виробничий процес. У роботі систематизовано основні загрози та вразливості цифрових двійників у середовищі CPS, зокрема підміну телеметрії, replay-атаки, втручання в модель, несанкціонований доступ, атаки на доступність, компрометацію каналів зв'язку, адміністративних сервісів і журналів подій. Проаналізовано криптографічні, мережеві, організаційні й прикладні механізми захисту, а також обґрунтовано необхідність їх інтеграції в багаторівневу архітектуру безпеки, побудовану з урахуванням принципів defense-in-depth і Zero Trust. Запропонована модель поєднує захист транспортного каналу, перевірку цілісності й автентичності повідомлень, протидію replay-атакам, контроль доступу, захищене журналювання з контролем цілісності записів, обмеження інтенсивності надходження повідомлень, валідацію телеметрії та модельно-орієнтований контроль стану цифрового двійника на основі оцінювання узгодженості між виміряним і прогнозованим станом. Практичну реалізацію виконано у вигляді програмного прототипу на основі Python, MQTT і Node-RED. У межах експериментальної перевірки відтворено контрольовані сценарії нормального функціонування та типових загроз, що дозволило оцінити реакцію системи на модифікацію повідомлень, повторне відтворення пакетів, аномальні телеметричні значення, неузгодженість із модельним станом, надлишковий потік повідомлень і спроби несанкціонованого адміністративного доступу. Отримані результати показали, що запропонований підхід забезпечує виявлення типових порушень, коректне відхилення аномальних або модифікованих повідомлень, підтримання контрольованої доступності сервісів і додаткову перевірку достовірності телеметрії на рівні моделі, що підтверджує практичну придатність розробленої моделі для побудови захищених цифрових двійників у контексті Industry 4.0.

Ключові слова: цифровий двійник; кіберфізична система; Industry 4.0; кіберзахист; модельно-орієнтований контроль; телеметрія; виявлення аномалій; MQTT.

ВСТУП

Сучасний етап розвитку промисловості пов'язаний із широким упровадженням концепції Industry 4.0, у межах якої кіберфізичні системи забезпечують тісну взаємодію фізичних процесів із цифровими платформами, мережевими сервісами, засобами аналітики та автоматизованого керування. Однією з ключових технологій цього середовища є цифровий двійник, який забезпечує цифрове представлення фізичного об'єкта, процесу або системи на основі безперервного надходження, оброблення та

інтерпретації даних. Поєднання цифрових двійників із IIoT, хмарними сервісами, алгоритмами аналізу даних і засобами диспетчеризації відкриває широкі можливості для моніторингу стану обладнання, прогнозування відмов, оптимізації виробничих режимів і підтримки прийняття рішень у режимі, наближеному до реального часу.

Разом із розширенням функціональних можливостей цифрових двійників зростає і їх значення як об'єктів кіберзахисту. На відміну від звичайних інформаційних систем, цифровий двійник інтегрований у кіберфізичний контур і взаємодіє з телеметрією, каналами передавання даних, прикладними сервісами, інтерфейсами керування та аналітичними модулями. За таких умов компрометація цифрового двійника не обмежується порушенням конфіденційності або доступності даних, а може призводити до формування хибних уявлень про стан фізичного об'єкта, втрати довіри до телеметрії, спотворення моделей і прийняття небезпечних рішень у виробничому середовищі.

Специфіка цифрового двійника як складника CPS полягає в тому, що для нього критичними є не лише конфіденційність і контроль доступу, а насамперед цілісність, своєчасність і достовірність даних [1]. Захищений канал зв'язку або коректна автентифікація не гарантують, що отримана телеметрія відповідає реальному стану фізичного процесу. Саме тому захист цифрових двійників потребує поєднання класичних механізмів кібербезпеки з контролем логічної та фізичної узгодженості між виміряним і прогнозованим станом системи.

Попри активний розвиток Digital Twin як технології Industry 4.0, питання її комплексного захисту залишаються недостатньо опрацьованими. У більшості випадків для побудови безпечного середовища цифрового двійника використовують адаптовані підходи із захисту IT- та OT-систем, тоді як специфіка двосторонньої взаємодії фізичного і цифрового контурів вимагає окремого узгодженого підходу [2]. За таких умов дослідження методів і засобів захисту цифрових двійників у кіберфізичних системах Industry 4.0 набуває безпосереднього теоретичного і практичного значення.

Постановка проблеми. Аналіз сучасних загроз у середовищі CPS свідчить, що цифровий двійник є багаторівневим об'єктом атаки, уразливим до підміни та фальсифікації телеметрії, replay-атак, втручання в моделі та алгоритми, компрометації каналів зв'язку, прикладних інтерфейсів, сервісів адміністрування, а також атак на доступність [4, 5]. У таких умовах захист, зведений лише до транспортного шифрування або периметрових засобів безпеки, не забезпечує належного рівня довіри до даних і стану цифрового двійника [6]. Особливої складності набуває виявлення формально коректних, проте недостовірних телеметричних повідомлень, які проходять криптографічну перевірку, але не відповідають реальній динаміці фізичного об'єкта. Отже, актуальним завданням є формування узгодженої моделі захисту цифрового двійника, яка поєднувала б криптографічні, мережеві, прикладні та модельно-орієнтовані механізми, забезпечувала б виявлення типових загроз і підтримувала б контроль достовірності телеметрії в межах єдиного програмного середовища.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі цифровий двійник переважно розглядають як цифрове представлення фізичного об'єкта, процесу або системи, що функціонує на основі двостороннього обміну даними та синхронізації фізичного й цифрового станів. Такий підхід сформував методологічну основу для розвитку цифрових двійників у промисловому виробництві, енергетиці, логістиці та інфраструктурних системах [7]. Разом із тим у значній частині досліджень цифровий двійник описується переважно як архітектурна або сервісна концепція без достатньої формалізації його стану як об'єкта контролю, що ускладнює побудову механізмів виявлення неузгодженостей між телеметрією та поведінкою моделі.

Окремий напрям досліджень присвячено аналізу загроз і вразливостей цифрових двійників у середовищі кіберфізичних систем [3-5]. У наукових працях розглядаються підміна телеметрії, false data injection, replay-атаки, втручання в модель, компрометація каналів IIoT-взаємодії, атаки типу «людина посередині», порушення часової синхронізації, несанкціонований доступ, атаки на доступність, а також ризики, пов'язані з хмарними сервісами, ланцюгом постачання та людським фактором [6, 8]. Ці дослідження підтверджують, що цифровий двійник не може розглядатися лише як прикладний сервіс оброблення даних, оскільки його компрометація здатна поширюватися на весь кіберфізичний контур.

У сучасній літературі також широко представлені праці, присвячені криптографічному захисту даних, автентифікації, керуванню доступом, журналюванню, моніторингу, IDS/IPS, SIEM, EDR/XDR, secure SDLC та захисту ланцюга постачання програмного забезпечення. Зазначені підходи формують важливу методичну основу для побудови захищених платформ Industry 4.0. Водночас більшість із них орієнтована або на окремі класи загроз, або на окремі технологічні шари системи. Недостатньо дослідженим залишається підхід, у межах якого криптографічні, мережеві, прикладні та модельно-орієнтовані механізми об'єднуються в єдину архітектуру захисту цифрового двійника з подальшою програмною реалізацією та експериментальною перевіркою її працездатності [7].

Мета статті. Метою статті є узагальнення сучасних методів і засобів захисту цифрових двійників у кіберфізичних системах Industry 4.0, систематизація характерних загроз і вразливостей, а також розроблення й експериментальна перевірка багаторівневої моделі кіберзахисту цифрового двійника, яка поєднує захист транспортного каналу, контроль цілісності й автентичності повідомлень, протидію replay-атакам, контроль доступу, журналювання, валідацію телеметрії та модельно-орієнтований контроль стану.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах дослідження захист цифрового двійника розглянуто як комплексне завдання, що охоплює формування вимог безпеки, побудову багаторівневої архітектури захисту, розроблення алгоритмічних механізмів протидії загрозам і їх подальшу програмну реалізацію. Такий підхід зумовлений тим, що цифровий двійник у складі кіберфізичної системи виконує не лише функції збирання та оброблення телеметрії, а й бере участь у моделюванні стану фізичного об'єкта, підтримці аналітики та формуванні рішень у режимі, наближеному до реального часу. За таких умов його захист не може обмежуватися окремими криптографічними або мережевими засобами, а потребує узгодженої архітектури, у межах якої поєднуються превентивні, детективні та відновлювальні механізми.

1. Формування вимог безпеки та архітектури захисту цифрового двійника. Цифровий двійник у складі кіберфізичної системи Industry 4.0 розглядається не лише як програмний контур оброблення телеметрії, а як формалізована модель стану умовного технологічного вузла промислової системи, для якого в лабораторному прототипі контролюються два основні параметри – температура робочого середовища та тиск. Така постановка використовується не для відтворення конкретної виробничої установки, а для моделювання типового телеметричного контуру, у межах якого цифровий двійник синхронізується з фізичним об'єктом, отримує виміряні дані, прогнозує стан і виявляє відхилення.

Стан фізичного об'єкта системи в дискретний момент часу k задається вектором:

$$x_k = [T_k \quad P_k]^T \tag{1}$$

де x_k – вектор стану об'єкта в момент часу k ; T_k – значення температури в момент часу k; P_k – значення тиск у момент часу k; $(\cdot)^T$ – операція транспортування.

Еволюція стану об'єкта описується рівнянням:

$$x_{k+1} = Ax_k + w_k, \tag{2}$$

де x_{k+1} – вектор стану об'єкта в наступний момент часу; A – матриця переходу стану, яка описує динаміку зміни параметрів об'єкта; w_k – вектор збурень процесу, що враховує невизначеність моделі, зовнішні впливи та випадкові відхилення.

Телеметричні дані, що надходять від сенсора до цифрового двійника, описуються рівнянням:

$$y_k = x_k + v_k, \tag{3}$$

де y_k – вектор виміряних телеметричних значень у момент часу k; v_k – вектор похибки вимірювання, який враховує шум сенсора, похибки передавання або спотворення даних.

Для оцінювання узгодженості між виміряним станом фізичного об'єкта та станом, прогнозованим цифровим двійником, обчислюється залишок:

$$r_k = y_k - \hat{x}_k, \tag{4}$$

де r_k – вектор залишку в момент часу k; $\hat{x}_k$ – оцінений або прогнозований цифровим двійником вектор стану об'єкта в момент часу k.

Ознакою аномалії вважається перевищення залишком встановленого порогового значення:

$$\|r_k\| > \gamma, \tag{5}$$

де $\|r_k\|$ – норма вектору залишку, що характеризує величину відхилення між виміряним і прогнозованим станами; γ – граничне порогове значення, перевищення якого свідчить про неузгодженість між фізичним і цифровим контурами та дає підстави розглядати подію як аномальну.

Така постановка дозволяє використовувати математичну модель не лише для відображення стану об'єкта, а і як механізм додаткового контролю достовірності телеметрії, що особливо важливо в умовах можливих атак на сенсорний рівень, канал передавання або цифровий контур оброблення даних.

Формування вимог безпеки для цифрового двійника ґрунтується на тому, що його компрометація впливає не тільки на інформаційний контур, а й на фізичний процес [2]. Тому базовими вимогами є конфіденційність, цілісність, доступність, автентичність, контроль доступу, підзвітність, простежуваність дій і можливість відновлення після інциденту. Для цифрового двійника визначальною є також довіра до даних, тобто гарантування їх походження, незмінності та своєчасності від моменту збирання до використання в аналітичних і керувальних модулях [3]. Саме порушення цих властивостей створює ризик формування хибних рішень у цифровому та фізичному контурах.

Вимога конфіденційності передбачає захист телеметрії, конфігурацій, журналів подій, моделей і службових повідомлень під час передавання та зберігання. Для цього доцільно використовувати TLS не нижче версії 1.2 з пріоритетом TLS 1.3, а на прикладному рівні – AEAD-схеми, зокрема AES-GCM. Вимога цілісності охоплює захист телеметрії, команд, конфігурацій, моделей і журналів від підміни, тому архітектура повинна передбачати MAC/HMAC, цифрові підписи, перевірку походження артефактів, контроль версій і захищене зберігання. Для цифрового двійника цього недостатньо без зіставлення отриманих значень із прогнозованим станом моделі, оскільки навіть захищений канал зв'язку не гарантує правильності показників у разі компрометації сенсора або проміжного сервісу.

Вимога доступності означає стабільне функціонування цифрового двійника за умов часткових збоїв, перевантажень або атак на доступність [4]. Це потребує сегментації мережі, фільтрації трафіку, резервування компонентів, лімітування запитів, ізоляції критичних сервісів і підготовлених механізмів локалізації DoS- та DDoS-впливів. Для промислового середовища важливою є також кіберрезильєнтність, тобто здатність системи повертатися до останнього довіреного стану після інциденту. Тому в архітектурі мають бути передбачені офлайн- або ізольовані резервні копії, незмінювані сховища та регулярне тестування процедур відновлення.

Автентичність і авторизація доступу повинні забезпечувати безпечну взаємодію як користувачів, так і пристроїв. Для користувачів доцільно застосовувати багатофакторну автентифікацію, для критичних операцій – фішингостійкі механізми, зокрема FIDO2/WebAuthn, а для сервісів і пристроїв – взаємну автентифікацію на основі X.509-сертифікатів і PKI. Контроль доступу доцільно реалізовувати за моделями RBAC або ABAC з дотриманням принципу найменших привілеїв. Для веб- і API-взаємодій раціонально використовувати OpenID Connect поверх OAuth 2.0 із застосуванням Authorization Code Flow з PKCE.

До обов'язкових складових архітектури належать моніторинг, журналювання та виявлення аномалій. Система має реєструвати суттєві події безпеки, зміни конфігурації, доступ до моделей і даних, спроби входу, API-виклики та підключення пристроїв. Журнали повинні централізовано збиратися, захищатися від прихованої модифікації та передаватися до SIEM для кореляції подій. Поряд із цим доцільно використовувати IDS/IPS і EDR/XDR, а також включати безпеку в життєвий цикл розроблення платформи цифрового двійника через secure SDLC із застосуванням SAST, DAST і SCA. Це дає змогу зменшити ризики ін'єкційних вразливостей, небезпечної обробки вхідних даних, помилок десеріалізації та компрометації сторонніх пакетів.

З урахуванням сформованих вимог архітектуру системи захисту цифрового двійника доцільно проєктувати на основі принципів defense-in-depth і Zero Trust. Вона повинна охоплювати захищений комунікаційний шлюз між фізичним рівнем і платформою цифрового двійника, модуль криптографічного захисту й управління ключами, модуль автентифікації та контролю доступу, підсистему журналювання й аудиту, засоби моніторингу та виявлення аномалій, контур захисту кінцевих вузлів, резервування та відновлення, а також модуль математичної моделі цифрового двійника, який відповідає за прогнозування стану та оцінювання залишку r_k [2]. Така побудова забезпечує не лише запобігання інцидентам, а й своєчасне виявлення неузгодженостей між фізичним і цифровим контурами та відновлення системи до довіреного стану [3]. Запропоновану багаторівневу архітектуру захисту цифрового двійника наведено на рис. 1.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

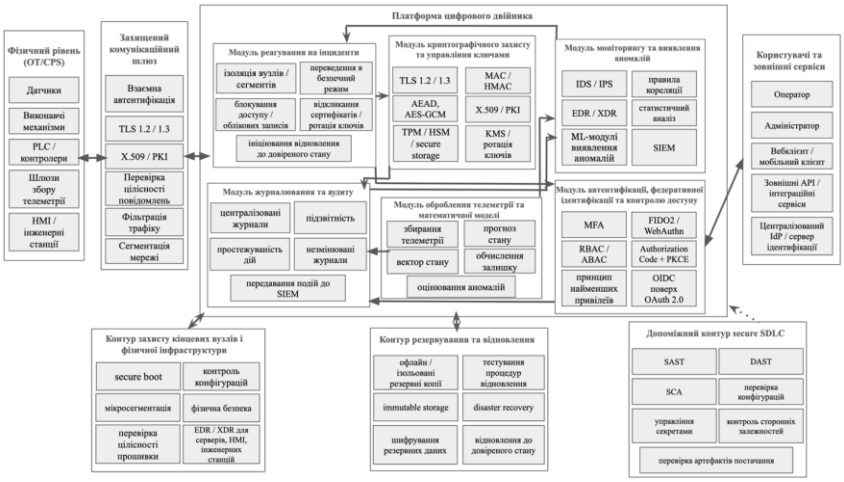


Рис. 1. Багаторівнева архітектура захисту цифрового двійника в кіберфізичній системі Industry 4.0

2. Розроблення алгоритмічних механізмів протидії загрозам. Алгоритмічні механізми протидії загрозам цифрового двійника розроблено за принципом багаторівневого захисту, за якого кожен критичний ризик покривається сукупністю превентивних, детективних і відновлювальних заходів. При цьому увага зосереджена на механізмах, що безпосередньо реалізують виявлення і нейтралізацію загроз. У межах даного дослідження цифровий двійник розглядається як модель стану умовного технологічного вузла кіберфізичної системи, для якого в лабораторному прототипі контролюються два основні телеметричні параметри – температура робочого середовища та тиск, що надалі використовуються для валідації телеметрії та оцінювання узгодженості між фізичним і цифровим станами.

Базовим алгоритмічним механізмом є модельно-орієнтований контроль телеметрії. Після отримання повідомлення виконується перевірка його криптографічної цілісності та часових атрибутів, після чого обчислюється залишок між виміряним вектором стану y_k і прогнозованим станом $\hat{x}_k$. Якщо виконується умова $\|r_k\| > \gamma$, то подія позначається як аномальна і передається до підсистем журналювання, моніторингу та реагування на інциденти. Для даного об'єкта компонентами векторів y_k та $\hat{x}_k$ виступають насамперед температура і тиск. Перевага цього підходу полягає в тому, що система спирається не лише на коректність каналу зв'язку та автентичність джерела повідомлення, а й на оцінювання узгодженості між фізичним і цифровим контурами. Саме тому він дає змогу виявляти replay-атаки, підміну телеметрії та інші неузгодженості навіть у випадках, коли повідомлення формально проходить криптографічну перевірку.

Для протидії атакам на доступність, насамперед DoS і DDoS, доцільно використовувати поєднання мережевої фільтрації, rate limiting, сегментації, резервування ресурсів, розподіленого розгортання сервісів і виявлення аномалій трафіку. Додатковий захисний ефект забезпечує декомпозиція платформи цифрового двійника з винесенням окремих функцій на крайові або дубльовані вузли, що зменшує ризик формування єдиної точки відмови. У разі виявлення flood-атаки засоби IDS/IPS або інші компоненти моніторингу повинні ініціювати автоматичне блокування джерела трафіку, переведення окремих сервісів у захищений режим або зміну маршрутизації трафіку.

Для нейтралізації атак типу MitM і компрометації каналу зв'язку між фізичним контуром і цифровим двійником алгоритм захисту має передбачати використання TLS 1.2/1.3, взаємну автентифікацію вузлів на основі X.509-сертифікатів, перевірку довіри до сертифікатів і застосування лише стійких наборів шифрів. Для критичних повідомлень транспортний захист доцільно доповнювати MAC/HMAC або цифровими підписами. У випадку підміни, фальсифікації та повторного відтворення даних до цього додаються часові мітки, nonce або порядкові номери, валідація фізичної правдоподібності телеметрії та аналіз залишку r_k. Навіть коректно підписані дані повинні позначатися як підозрілі, якщо вони виходять за межі допустимого технологічного профілю або формують надмірне відхилення від прогнозованої динаміки.

Для прикладного рівня критичними залишаються атаки на вебінтерфейси, API та механізми оброблення повідомлень. Тому алгоритмічні механізми захисту повинні включати сувору валідацію вхідних даних, перевірку схеми й типів, параметризовані запити, контекстно-залежне екранування, контроль origin для WebSocket-з'єднань, застосування WAF і заборону небезпечної десеріалізації. Вхідні повідомлення не повинні передаватися до логіки цифрового двійника без перевірки формату, допустимих діапазонів і контексту використання. У контексті розробленого прототипу це означає

обов'язковий контроль наявності телеметричних полів, коректності числового типу, допустимих меж температури і тиску та максимально припустимого приросту значень між сусідніми повідомленнями. Цей клас захисту безпосередньо пов'язаний із secure SDLC, оскільки саме на етапі розроблення усувається значна частина ін'єкційних і десеріалізаційних ризиків.

Окрему групу становлять механізми протидії зловживанню доступом, компрометації облікових записів і внутрішнім загрозам. Для цього використовуються фішингостійка MFA, моделі RBAC/ABAC, принцип найменших привілеїв, PAM, блокування після невдалих спроб входу, перевірка паролів за списками скомпрометованих значень, журналювання критичних дій, поведінкова аналітика користувачів і сутностей, сегментація та регулярний перегляд прав доступу [3]. Для зовнішніх інтеграцій доцільно застосовувати OpenID Connect поверх OAuth 2.0 з Authorization Code Flow + PKCE. Такий набір механізмів зменшує ймовірність як зовнішньої компрометації акаунтів, так і зловживання привілеями всередині системи.

Для цифрових двійників необхідно враховувати також ризики фішингу, ransomware, компрометації ланцюга постачання, отруєння навчальних даних і витоку через модель [9]. У цих випадках алгоритм протидії повинен поєднувати навчання персоналу, фільтрацію електронної пошти, sandbox-аналіз вкладень, офлайн- або ізольовані резервні копії, immutable storage, тестування відновлення, SCA, SBOM, перевірку provenance, контроль CI/CD, валідацію навчальних наборів, розмежування train- і prod-середовищ, обмеження доступу до параметрів моделі та аудит запитів до модельних API. Для цифрового двійника це особливо важливо, оскільки втручання в алгоритмічні модулі або навчальні дані знижує достовірність прогнозів навіть за відсутності явного збою системи [10].

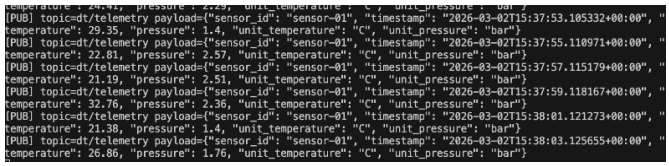
Таблиця 1

Відповідність типових загроз цифровому двійнику та механізмів їх нейтралізації

Загроза	Механізм протидії	Очікуваний результат
MitM	Перехоплення телеметрії, підміна команд, десинхронізація між об'єктом і моделлю	Захищений транспортний канал; взаємна автентифікація вузлів; контроль цілісності повідомлень
Підміна даних / replay-атака	Спотворення стану цифрового двійника, хибні рішення, ризик для фізичного процесу	Часові мітки; nonce; порядкові номери; валідація телеметрії; модельно-орієнтований контроль залишку
Аномальні або сфальсифіковані дані телеметрії	Валідація структури, діапазону і дельти параметрів, модельно-орієнтований контроль залишку	Виявлення недостовірних даних, що не відповідають очікуваному стану об'єкта
Несанкціонований доступ	Компрометація акаунтів, витік даних, порушення роботи API і сервісів	MFA; RBAC / ABAC; принцип найменших привілеїв; контроль критичних дій
DoS / DDoS	Відмова в обслуговуванні, затримка телеметрії, втрата доступності сервісів	Rate limiting; фільтрація трафіку; сегментація; резервування ресурсів; виявлення аномалій трафіку
Ін'єкційні та прикладні атаки на API / вебінтерфейс	Виконання небажаного коду, викрадення токенів, компрометація логіки сервісу	Валідація вхідних даних; schema validation; параметризовані запити; secure SDLC
Внутрішні зловживання та приховані зміни	Прихована зміна моделей, конфігурацій або даних	Журналювання; аудит; перегляд прав доступу; контроль цілісності записів
Фішинг / соціальна інженерія	Компрометація облікових даних, початковий доступ до інфраструктури	Навчання персоналу; фільтрація пошти; sandbox-аналіз вкладень; фішингостійка MFA
Ransomware /післяінцидентний збій	Шифрування даних, зупинення сервісів, втрата відновлюваності	Ізольовані резервні копії; незмінювані сховища; тестування відновлення
Компрометація supply chain	Впровадження шкідливого коду, ризик для CI/CD і сторонніх залежностей	SCA; SBOM; перевірка походження артефактів; контроль сторонніх залежностей
Model poisoning / model inversion	Спотворення прогнозів, витік чутливих параметрів або даних	Валідація навчальних даних; розмежування train/prod; контроль доступу до моделей; аудит запитів

3. Програмна реалізація функціональних модулів захисту. Програмну реалізацію запропонованих функціональних модулів виконано у вигляді лабораторного прототипу цифрового двійника, побудованого на основі Python, MQTT і Node-RED [11]. У межах прототипу фізичний рівень кіберфізичної системи представлено емулятором сенсора, який формує телеметричні повідомлення у форматі JSON, а програмні модулі приймання, перевірки та журналювання реалізовано на стороні цифрового контуру. У даному випадку цифровий двійник моделює стан умовного технологічного вузла кіберфізичної системи, для якого контролюються два основні параметри – температура робочого середовища та тиск. Така побудова дала змогу поетапно інтегрувати функціональні модулі захисту та простежити їх роботу в єдиному середовищі.

На початковому етапі реалізації сформовано базовий контур передавання телеметричних даних між емулятором фізичного об’єкта та цифровим двійником. Для цього в середовищі Python реалізовано модуль sensor, який генерує поточні значення температури і тиску контрольованого технологічного вузла та формує телеметричне повідомлення у форматі JSON. Передавання повідомлень організовано через MQTT-брокер із використанням топіка dt/telemetry (рис. 2). Публікацію телеметрії виконує окремий модуль publisher, який встановлює з’єднання з брокером і періодично передає сформовані повідомлення. У результаті реалізації створено працездатний канал обміну даними між джерелом телеметрії та приймальною стороною, який використано як базу для подальшого інтегрування функціональних модулів захисту.

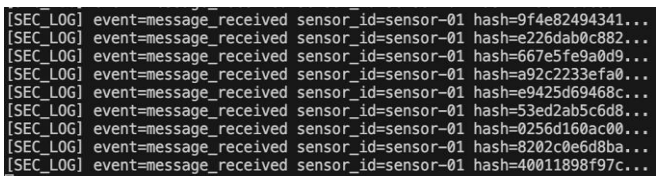


а)

б)

Рис. 2. Передавання телеметричних повідомлень від емулятора сенсора до MQTT-брокера в лабораторному прототипі цифрового двійника: а) формування повідомлень на стороні відправника; б) надходження повідомлень до топіка dt/telemetry

Після формування базового каналу передавання даних у прототип було інтегровано приймальний шлюз оброблення телеметрії gateway, який підписується на MQTT-топік dt/telemetry і виконує реєстрацію отриманих подій. На цьому етапі реалізовано модуль захищеного журналювання SEC Log, що формує записи у форматі JSONL для кожного прийнятого повідомлення (рис. 3). До складу запису включено часову мітку, тип події, статус оброблення, ідентифікатор джерела, назву топіка, стислий опис вмісту повідомлення та службову причину прийнятого рішення. Для контролю цілісності журналу до структури запису додано поля prev_hash і hash, за рахунок яких формується хеш-ланцюжок між послідовними записами. У результаті кожне повідомлення, прийняте шлюзом, супроводжується створенням окремого журнального запису, придатного для аудиту та подальшої перевірки цілісності.

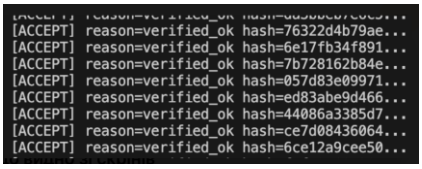


а)

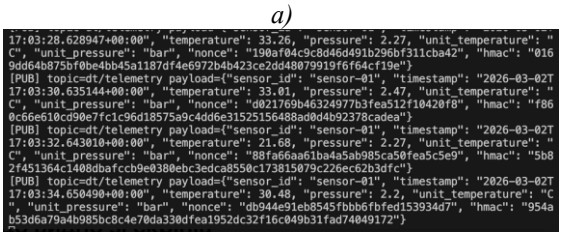
(б)

Рис. 3. Реалізація захищеного журналювання в лабораторному прототипі цифрового двійника: а) формування записів SEC Log у приймальному шлюзі; б) фрагмент файлу sec_log.jsonl із полями prev_hash і hash

Наступним кроком стало впровадження модуля контролю цілісності й автентичності телеметричних повідомлень (рис. 4). Його реалізовано як сукупність двох програмних компонентів – модуля publisher, що формує підписане повідомлення, і модуля gateway, який виконує його перевірку. На стороні відправника до структури телеметричного повідомлення додано службові поля timestamp, nonce і hmac. Поле timestamp містить часову мітку формування повідомлення, nonce – одноразовий ідентифікатор пакета, а hmac – криптографічний підпис, обчислений від вмісту повідомлення до його передавання через MQTT-канал. На стороні приймального шлюзу реалізовано послідовну процедуру перевірки, яка охоплює контроль наявності службових полів, перевірку актуальності часової мітки, перевірку унікальності nonce та повторне обчислення HMAC-підпису для зіставлення з отриманим значенням. Повідомлення, що успішно проходять усі етапи перевірки, позначаються як коректні та реєструються в журналі подій, тоді як повідомлення з порушеною структурою або невідповідністю контрольних значень відхиляються на рівні приймального шлюзу.



а)



б)

Рис. 4. Реалізація контролю цілісності й автентичності телеметричних повідомлень: а) успішна перевірка повідомлень у приймальному шлюзі; б) структура підписаного повідомлення з полями timestamp, nonce і hmac

Наступним компонентом, інтегрованим у приймальний шлюз лабораторного прототипу, є модуль валідації телеметрії, реалізований як окремий програмний компонент перевірки вхідних повідомлень. Після успішного проходження криптографічної перевірки модуль виконує контроль наявності полів temperature і pressure, перевірку їх числового типу, а також зіставлення отриманих значень із заданими межами TEMP_MIN, TEMP_MAX, PRESSURE_MIN і PRESSURE_MAX. Додатково реалізовано перевірку максимально допустимої зміни температури між сусідніми повідомленнями за параметром DELTA_TEMP_MAX. Якщо хоча б одна з умов не виконується, повідомлення відхиляється на етапі приймання, а відповідна причина фіксується в журналі подій. У результаті до подальшої логіки цифрового двійника передаються лише повідомлення, що пройшли як криптографічну, так і змістовну перевірку.

Після реалізації базової валідації телеметрії до складу приймального шлюзу було інтегровано модуль перевірки узгодженості між виміряним і прогнозованим станом цифрового двійника. Його програмну реалізацію виконано у вигляді окремого компонента ModelConsistencyChecker, який використовує поточне та попереднє значення стану для формування прогнозованих параметрів температури й тиску (рис. 5). На основі різниці між отриманими та прогнозованими значеннями обчислюється нормалізований залишок residual. Якщо величина залишку не перевищує встановлені

порогові значення, повідомлення позначається як узгоджене з моделлю та допускається до подальшої обробки. У протилежному випадку повідомлення має бути відхилене як аномальне. Така програмна реалізація дозволяє доповнити криптографічну і формальну перевірку телеметрії оцінюванням її поведінкової узгодженості в межах цифрового двійника.

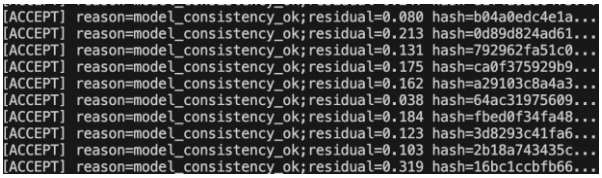


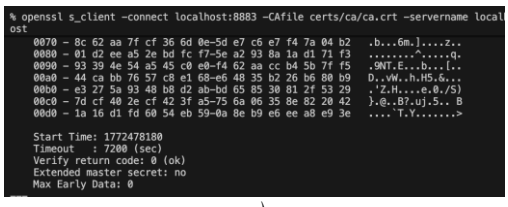
Рис. 5. Результати роботи модуля Model Consistency Checker у нормальному режимі

Наступним компонентом, інтегрованим у приймальний шлюз лабораторного прототипу, є модуль обмеження частоти повідомлень RateLimiter. Його програмну реалізацію виконано як окремий компонент контролю інтенсивності надходження телеметрії, який відстежує кількість повідомлень, отриманих від джерела протягом заданого часового вікна. Перевірка виконується на початковому етапі оброблення повідомлення, до запуску подальших процедур криптографічної та змістовної перевірки. Якщо кількість повідомлень у межах встановленого інтервалу не перевищує заданого порога, телеметрія передається до наступних модулів оброблення. У разі перевищення ліміту повідомлення має бути відхилене на рівні приймального шлюзу з реєстрацією причини в журналі подій. Така програмна реалізація дозволяє обмежити надлишковий потік телеметрії та підготувати основу для експериментальної перевірки стійкості системи до перевантаження вхідного каналу.

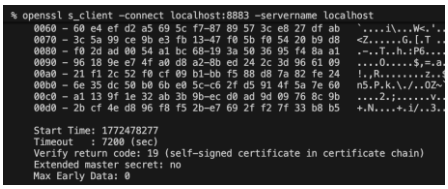
У межах лабораторного прототипу захист адміністративного доступу до середовища Node-RED реалізовано за допомогою механізму adminAuth у файлі конфігурації settings.js. Для цього створено два облікові записи з різними рівнями доступу – користувача admin із повними правами керування та користувача operator із правами лише читання. Паролі збережено у вигляді bcrypt-хешів, а розмежування дозволів виконано на рівні вбудованої системи авторизації Node-RED. Така реалізація забезпечує базовий контроль доступу до редактора потоків і зменшує ризик несанкціонованої зміни логіки оброблення телеметрії.

4. Аналіз ефективності функціонування програмної моделі кіберзахисту DT. Ефективність функціонування розробленої програмної моделі кіберзахисту цифрового двійника оцінювалась у межах лабораторного експерименту шляхом відтворення контрольованих сценаріїв оброблення телеметрії та типових кіберзагроз. Перевірку виконано для всіх реалізованих функціональних модулів захисту, інтегрованих у програмний прототип, зокрема захищеного транспортного каналу MQTT over TLS, модуля контролю цілісності й автентичності повідомлень на основі HMAC, механізму протидії replay-атакам із використанням timestamp і nonce, модуля валідації телеметрії, модуля перевірки узгодженості між виміряним і прогнозованим станом, модуля обмеження частоти повідомлень, захищеного журналювання SEC Log та механізму контролю адміністративного доступу в Node-RED. Оцінювання здійснювалось за реакцією приймального шлюзу, записами журналу подій і результатами виконання тестових сценаріїв, у межах яких фіксувались фактична поведінка системи, причини прийняття або відхилення повідомлень і здатність окремих модулів виявляти порушення вхідного потоку даних.

Першим етапом експериментальної перевірки було оцінювання працездатності захищеного транспортного каналу MQTT over TLS (рис. 6). Для цього виконано два контрольовані сценарії: встановлення з’єднання з використанням довіреного сертифікаційного центру CA та спробу перевірки серверного сертифіката без його використання. У першому випадку верифікація завершилась успішно, що підтверджувалось результатом Verify return code: 0 (ok). У другому випадку перевірка сертифіката не пройшла, що супроводжувалось повідомленням Verify return code: 19 (self-signed certificate in certificate chain). Це засвідчило, що коректна робота захищеного транспортного каналу в розробленому прототипі залежить від наявності довіри до серверного сертифіката.



а)

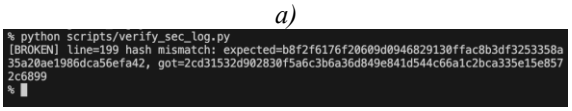


б)

Рис. 6. Експериментальна перевірка захищеного транспортного каналу MQTT over TLS: а) успішна верифікація серверного сертифіката з використанням довіреного CA; б) помилка перевірки сертифіката без використання довіреного CA

Наступним етапом експериментальної перевірки було оцінювання працездатності модуля захищеного журналювання SEC Log (рис. 7). Спочатку журнал перевірено в коректному стані, у якому скрипт верифікації підтвердив цілісність усіх записів і правильність хеш-ланцюжка. Після цього один із попередніх записів журналу було навмисно змінено вручну без перерахунку контрольних значень. Повторна перевірка виявила порушення цілісності журналу, що супроводжувалось повідомленням про невідповідність хешу або розрив зв'язку між послідовними записами. Експеримент показав, що реалізований механізм SEC Log дозволяє виявляти приховану модифікацію журналу подій.

а)



б)

Рис. 7. Експериментальна перевірка цілісності журналу SEC Log: а) успішна верифікація хеш-ланцюжка в початковому стані; б) виявлення порушення цілісності після ручної модифікації запису

Наступним етапом експериментальної перевірки було оцінювання модуля контролю цілісності й автентичності телеметричних повідомлень. Для цього сформовано тестовий сценарій, у межах якого після обчислення HMAC-підпису навмисно змінювалось одне з полів телеметричного повідомлення (рис. 8). У результаті приймальний шлюз повторно обчислював контрольне значення та виявляв його невідповідність отриманому підпису, після чого повідомлення відхилялося з ознакою hmac_invalid. Це підтвердило, що реалізований механізм HMAC Protection дозволяє виявляти підміну телеметричних даних після формування підпису та унеможливлює їх подальше приймання системою.

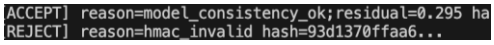


Рис. 8. Результат експериментальної перевірки модуля HMAC Protection: відхилення телеметричного повідомлення з порушеною цілісністю

Окремим етапом експериментальної перевірки було оцінювання механізму протидії replay-атакам. Для цього те саме телеметричне повідомлення з незмінними значеннями timestamp, nonce і hmac було надіслано двічі (рис. 9). Під час першого надсилання повідомлення успішно проходило перевірки та приймалося системою. Повторне надсилання того самого пакета призводило до його відхилення на рівні приймального шлюзу з ознакою replay_detected, оскільки одноразовий ідентифікатор nonce уже був зафіксований у пам'яті системи. За результатами перевірки встановлено, що механізм Replay Protection забезпечує виявлення повторного відтворення раніше прийнятих повідомлень.

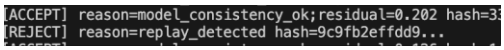


Рис. 9. Результат експериментальної перевірки механізму Replay Protection: відхилення повторно надісланого повідомлення з однаковим nonce

Для експериментальної перевірки модуля валідації телеметрії сформовано повідомлення з температурним значенням контрольованого технологічного вузла, що виходило за межі допустимого

діапазону. Повідомлення було коректно підписане та містило валідні службові поля, тому успішно проходило транспортну і криптографічну перевірку. Однак на етапі змістовної валідації приймальний шлюз виявляв невідповідність параметра температури встановленим межам і відхиляв повідомлення з ознакою temperature_out_of_range. Отримані дані підтвердили, що модуль Telemetry Validator дозволяє виявляти телеметричні дані, які формально є автентичними, але не відповідають заданим технологічним обмеженням.

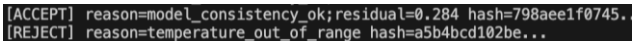


Рис. 10. Результат експериментальної перевірки модуля Telemetry Validator: відхилення телеметричного повідомлення з недопустимим значенням температури

Для перевірки модуля узгодженості між виміряним і прогнозованим станом було сформовано сценарій, у межах якого після серії узгоджених телеметричних повідомлень до приймального шлюзу надсилалися повідомлення з параметрами, що залишалися формально допустимими, але суттєво відхилялися від прогнозованого стану. У результаті шлюз обчислював нормалізований залишок residual і, у разі перевищення встановленого порогового значення, відхиляв повідомлення з ознакою model_residual_exceeded. Це засвідчило, що модуль Model Consistency Checker дозволяє виявляти телеметрію, яка проходить криптографічну і базову змістовну перевірку, але не узгоджується з поточним станом цифрового двійника (рис. 11).

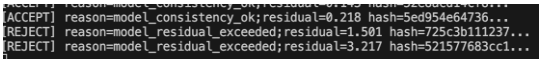
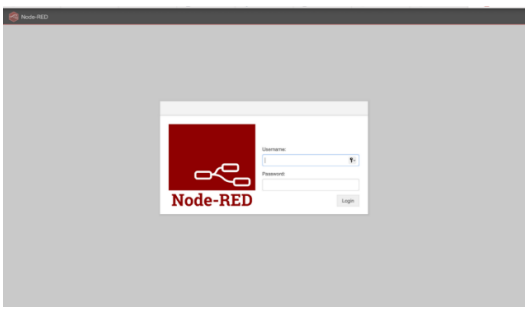


Рис. 11. Результат експериментальної перевірки модуля Model Consistency Checker: відхилення телеметричних повідомлень із перевищенням нормалізованого залишку residual

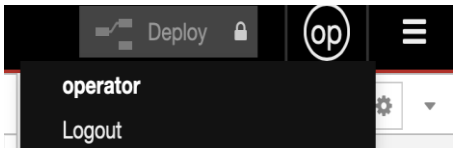
Для модуля обмеження частоти повідомлень було сформовано сценарій інтенсивного надсилання телеметрії від одного джерела в межах короткого часового інтервалу. Повідомлення передавалися з коректною структурою, валідним криптографічним підписом і допустимими параметрами стану, однак їх кількість перевищувала встановлений ліміт для заданого вікна часу. У результаті приймальний шлюз після досягнення порогового значення починав відхиляти наступні повідомлення з ознакою rate_limit_exceeded. Таким чином підтверджено працездатність реалізованого модуля RateLimiter і його здатність обмежувати надлишковий потік телеметрії на ранньому етапі оброблення (рис. 12).

Рис. 12. Результат експериментальної перевірки модуля RateLimiter: відхилення повідомлень у разі перевищення допустимої інтенсивності надходження телеметрії

Окремим етапом експериментальної перевірки було оцінювання механізму захисту адміністративного доступу до середовища Node-RED. Для цього виконано вхід до редактора потоків під обліковим записом operator, якому в конфігурації системи призначено права лише читання. У результаті доступ до середовища було надано без можливості повноцінної зміни логіки потоків, що підтвердило коректність розмежування ролей між користувачами admin і operator. Це засвідчило працездатність реалізованого механізму adminAuth і можливість обмеження адміністративних повноважень у межах лабораторного прототипу.



а)



б)

Рис. 13. Експериментальна перевірка механізму Node-RED adminAuth: а) форма автентифікації користувача в середовищі Node-RED; б) вхід під обліковим записом operator з обмеженими правами доступу

За результатами експериментальної перевірки встановлено, що розроблена програмна модель кіберзахисту цифрового двійника забезпечує коректне оброблення легітимної телеметрії та виявлення типових порушень на різних рівнях функціонування системи. Транспортний рівень захисту підтвердив працездатність за умови коректної довіри до сертифіката сервера, журналювання дозволило виявляти модифікацію записів, а прикладні модулі забезпечили виявлення підміни повідомлень, повторного відтворення пакетів, аномальних телеметричних значень, неузгодженості з модельним станом і надлишкового потоку повідомлень. Окремо підтверджено працездатність механізму розмежування адміністративного доступу в середовищі Node-RED.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У межах даного дослідження запропоновано комплексний підхід до побудови та оцінювання програмної моделі кіберзахисту цифрового двійника в кіберфізичних системах Industry 4.0, що поєднує транспортні, криптографічні, прикладні, модельно-орієнтовані та адміністративні механізми захисту. Розроблений підхід охоплює захищений транспортний канал MQTT over TLS, контроль цілісності й автентичності телеметричних повідомлень на основі HMAC, протидію replay-атакам із використанням timestamp і nonce, валідацію телеметрії, перевірку узгодженості між виміряним і прогнозованим станом, обмеження частоти повідомлень, захищене журналювання SEC Log і розмежування адміністративного доступу в середовищі Node-RED. Така побудова дозволяє розглядати цифровий двійник не лише як засіб моніторингу й аналітики, а як окремий об’єкт кіберзахисту, компрометація якого безпосередньо впливає на достовірність даних, стан моделей і безпеку фізичного процесу.

Реалізація запропонованої моделі у вигляді лабораторного прототипу на основі Python, MQTT і Node-RED підтвердила її прикладну придатність. Побудований прототип забезпечує послідовне проходження телеметричного повідомлення через ланцюг перевірок, у межах якого контролюються захищеність транспортного каналу, цілісність і автентичність повідомлення, коректність телеметричних параметрів, узгодженість із модельним станом та допустима інтенсивність надходження повідомлень. Додатково реалізовано захищене журналювання з хеш-ланцюжком, що створює можливість аудиту подій і виявлення прихованої модифікації журнальних записів. Експериментальна перевірка показала, що система коректно обробляє легітимну телеметрію та виявляє типові порушення, зокрема підміну даних, повторне відтворення повідомлень, аномальні значення параметрів, неузгодженість із прогнозованим станом, надлишковий потік телеметрії та спроби несанкціонованого адміністративного доступу.

Отримані результати свідчать, що програмна модель кіберзахисту цифрового двійника доцільно розглядати як багаторівневу систему, у якій криптографічні механізми мають доповнюватися перевіркою змістовної коректності й модельно-орієнтованим контролем стану. Саме таке поєднання дозволяє виявляти не лише формально некоректні повідомлення, а й дані, які мають валідну структуру та криптографічний підпис, але не відповідають поточній динаміці об’єкта або заданим технологічним обмеженням. Це підвищує достовірність функціонування цифрового двійника, зменшує ризик прийняття помилкових рішень на основі скомпрометованої телеметрії та формує практичну основу для побудови захищених цифрових контурів у контексті Industry 4.0.

Подальший розвиток дослідження доцільно зосередити на поглибленні модельно-орієнтованих методів контролю стану цифрового двійника, розширенні набору поведінкових ознак аномальності та підвищенні адаптивності механізмів виявлення порушень. Перспективним напрямом є застосування методів машинного навчання для побудови точніших прогнозних моделей стану, автоматичного налаштування порогових значень і врахування складнішої динаміки технологічних процесів. Окремої уваги потребує дослідження взаємодії між функціональними модулями захисту в умовах масштабованих цифрових двійників, де одночасно функціонують кілька джерел телеметрії, розподілені брокери повідомлень і декілька рівнів оброблення даних.

Перспективним є також розвиток інтеграції запропонованої моделі з практиками безпечної розробки, системами моніторингу інцидентів і промисловими засобами керування доступом. Це стосується автоматизації перевірок у CI/CD-контурах, розширення механізмів журналювання до рівня централізованого аудиту, а також поєднання цифрового двійника із засобами виявлення інцидентів у реальному часі. Практичну цінність становить і подальше дослідження засобів захисту адміністративного контуру, зокрема гнучкішого розмежування ролей, багатофакторної автентифікації та протоколювання змін конфігурації. Розвиток цих напрямів дозволить підвищити стійкість цифрових двійників до кіберзагроз і наблизити запропоновану модель до умов реальної експлуатації в кіберфізичних системах промислового призначення.

ПОДЯКА

This work was supported by a grant from the Simons Foundation International (SFI-PD-Ukraine-00014577; O.G.).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. El-Hajj, M., Itäpelto, T., & Gebremariam, T. (2024). Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Security and Privacy*. https://doi.org/10.1002/spy2.396
2. Voas, J., Mell, P., Laplante, P., & Piroumian, V. (2025). *Security and trust considerations for digital twin technology (NIST IR 8356)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8356
3. Zemskov, A. D., Fu, Y., Li, R., Wang, X., Karkaria, V., Tsai, Y.-K., Chen, W., Zhang, J., Gao, R., Cao, J., Loparo, K. A., & Li, P. (2024). Security and privacy of digital twins for advanced manufacturing: A survey [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2412.13939
4. Alhumam, N., Rahman, M. M. H., & Aljughaiman, A. (2025). A comprehensive review on cybersecurity of digital twins: Issues, challenges, and future research directions. *IEEE Access*. https://doi.org/10.1109/access.2025.3545004
5. Suárez-Román, M., Sanz-Rodrigo, M., Marín-López, A., & Arroyo, D. (2025). A digital twin threat survey. *Big Data and Cognitive Computing*, 9(10), Article 252. https://doi.org/10.3390/bdcc9100252
6. Zhang, H., Peng, S., Liu, L., Su, S., & Cao, Y. (2020). Review on GPS spoofing-based time synchronisation attack on power system. *IET Generation, Transmission & Distribution*, 14(20), 4301-4309. https://doi.org/10.1049/iet-gtd.2020.0253
7. Pilakkat, D., Balasubramanian, K., & Rajendran, S. R. (2025). Towards intelligent digital twins for PV systems: A unified framework for control, forecasting, and grid integration. *IEEE Access*. https://doi.org/10.1109/access.2025.3644889
8. Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, 8(2). https://doi.org/10.1002/spy2.70016
9. Zhang, Z., Fang, M., Chen, M., Li, G., Lin, X., & Liu, Y. (2024). Securing distributed network digital twin systems against model poisoning attacks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/jiot.2024.3421895
10. Homaei, M., Morales, V. G., Mogollon-Gutierrez, O., & Caro, A. (2025). The dark side of digital twins: Adversarial attacks on AI-driven water forecasting [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2504.20295
11. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of digital twins in dairy production. *Technology Audit and Production Reserves*, 2(2(82)), 37-49. https://doi.org/10.15587/2706-5448.2025.325422

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Tetiana Savchenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Informatics
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
ORCID: 0000-0002-8884-5360
tsavchenko@ukma.edu.ua

Sofiia Lapina
Student majoring in «Cybersecurity and Information Protection»
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine
ORCID: 0009-0006-5425-9984
s.lapina@ukma.edu.ua

METHODS AND TOOLS FOR PROTECTING DIGITAL TWINS IN INDUSTRY 4.0 CYBER-PHYSICAL SYSTEMS

Abstract. This article presents an integrated approach to the analysis, design, and practical implementation of digital twin protection in Industry 4.0 cyber-physical systems. The relevance of the study is determined by the fact that, in a modern industrial environment, a digital twin acts not only as a monitoring and analytics tool but also as a functional component of the digital loop, the compromise of which may lead to violations of telemetry integrity and reliability, loss of synchronization between physical and digital states, service degradation, and hazardous effects on the production process. The paper systematizes the main threats and vulnerabilities of digital twins in CPS environments, including telemetry tampering, replay attacks, model interference, unauthorized access, availability attacks, compromise of communication channels, administrative services, and event logs. Cryptographic, network, organizational, and application-level protection mechanisms are analyzed, and the need for their integration into a multilayer security architecture based on the principles of defense-in-depth and Zero Trust is substantiated. The proposed model combines transport channel protection, verification of message integrity and authenticity, replay-attack mitigation, access control, secure logging with log-integrity control, limitation of message arrival intensity, telemetry validation, and model-based monitoring of the digital twin state through the assessment of consistency between the measured and predicted states. The practical implementation is presented in the form of a software prototype based on Python, MQTT, and Node-RED. Within the experimental evaluation, controlled scenarios of normal operation and typical threats were reproduced, which made it possible to assess the system's response to message modification, packet replay, anomalous telemetry values, inconsistency with the model state, excessive message flow, and attempts at unauthorized administrative access. The obtained results showed that the proposed approach provides detection of typical violations, correct rejection of anomalous or modified messages, maintenance of controlled service availability, and additional verification of telemetry reliability at the model level, which confirms the practical applicability of the developed model for building secure digital twins in Industry 4.0 context.

Keywords: digital twin; cyber-physical system; Industry 4.0; cyber protection; model-based monitoring; telemetry; anomaly detection; MQTT.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. El-Hajj, M., Itäpelto, T., & Gebremariam, T. (2024). Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Security and Privacy*. https://doi.org/10.1002/spy2.396
2. Voas, J., Mell, P., Laplante, P., & Piroumian, V. (2025). *Security and trust considerations for digital twin technology (NIST IR 8356)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8356
3. Zemskov, A. D., Fu, Y., Li, R., Wang, X., Karkaria, V., Tsai, Y.-K., Chen, W., Zhang, J., Gao, R., Cao, J., Loparo, K. A., & Li, P. (2024). Security and privacy of digital twins for advanced manufacturing: A survey [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2412.13939

4. Alhumam, N., Rahman, M. M. H., & Aljughaiman, A. (2025). A comprehensive review on cybersecurity of digital twins: Issues, challenges, and future research directions. *IEEE Access*. https://doi.org/10.1109/access.2025.3545004
5. Suárez-Román, M., Sanz-Rodrigo, M., Marín-López, A., & Arroyo, D. (2025). A digital twin threat survey. *Big Data and Cognitive Computing*, 9(10), Article 252. https://doi.org/10.3390/bdcc9100252
6. Zhang, H., Peng, S., Liu, L., Su, S., & Cao, Y. (2020). Review on GPS spoofing-based time synchronisation attack on power system. *IET Generation, Transmission & Distribution*, 14(20), 4301-4309. https://doi.org/10.1049/iet-gtd.2020.0253
7. Pilakkat, D., Balasubramanian, K., & Rajendran, S. R. (2025). Towards intelligent digital twins for PV systems: A unified framework for control, forecasting, and grid integration. *IEEE Access*. https://doi.org/10.1109/access.2025.3644889
8. Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, 8(2). https://doi.org/10.1002/spy2.70016
9. Zhang, Z., Fang, M., Chen, M., Li, G., Lin, X., & Liu, Y. (2024). Securing distributed network digital twin systems against model poisoning attacks. *IEEE Internet of Things Journal*. https://doi.org/10.1109/jiot.2024.3421895
10. Homaei, M., Morales, V. G., Mogollon-Gutierrez, O., & Caro, A. (2025). The dark side of digital twins: Adversarial attacks on AI-driven water forecasting [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2504.20295
11. Savchenko, T., Lutska, N., Vlasenko, L., Sashnova, M., Zahorulko, A., Minenko, S., Ibaiev, E., & Tytarenko, N. (2025). Risk analysis and cybersecurity enhancement of digital twins in dairy production. *Technology Audit and Production Reserves*, 2(2(82)), 37-49. https://doi.org/10.15587/2706-5448.2025.325422

Отримано редакцією журналу / Received: 10.02.26
Прорецензовано / Revised: 25.02.26
Схвалено до друку / Accepted: 25.06.26