**ЛУНГОЛ Ольга,**
кандидат педагогічних наук, доцент,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ
(м. Кропивницький, Україна)
**МАКАРИНСЬКА Анна,**
рядовий поліції, курсант факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ
(м. Кропивницький, Україна)

## РОЗРОБКА ТА ЗАСТОСУВАННЯ КІБЕРФІЗИЧНИХ СИСТЕМ

Кіберфізична система (cyber-physical system – CPS) – це складна розподілена система, керована або контрольована комп'ютерними алгоритмами, тісно інтегрована з інтернетом і його користувачами [1]. Кіберфізичні системи поєднують фізичні та кібернетичні компоненти, щоб спільно керувати та контролювати фізичними процесами в реальному часі. У CPS фізичні об'єкти, такі як датчики, пристрої збірки даних та робочі механізми, взаємодіють із кібернетичними складовими, такими як комп'ютерні програми, алгоритми та мережі зв'язку. Це дозволяє системі спостерігати, аналізувати та реагувати на зміни в реальному середовищі, роблячи CPS основою для розумних систем управління, автоматизації та

моніторингу в різних галузях, таких як виробництво, транспорт, медицина та інфраструктура.

Кіберфізичні системи можуть бути частиною інжинірингового STEM-середовища. STEM визначає науку, технологію, інжиніринг та математику. Це дозволяє використовувати концепції та методи STEM для розробки, впровадження та управління кіберфізичними системами. Інжинірингове STEM-середовище в підготовці операторів складних систем може включати навчальні програми, лабораторні практикуми, дослідницькі проєкти та практичний досвід з роботи з кіберфізичними системами. Таким чином, вивчення кіберфізичних систем може бути важливою складовою інжинірингового STEM-середовища в підготовці операторів складних систем.

Застосування CPS охоплює широкий спектр галузей та сфер діяльності, де ці системи виявляються дуже корисними та ефективними. У сучасних виробничих умовах CPS використовуються для створення «розумного» виробництва, де обладнання й процеси автоматизовані та зв'язані мережею для оптимізації виробничих процесів, підвищення продуктивності та зменшення витрат. У сучасних автомобілях використовуються CPS для реалізації систем автоматизованого управління, водіння в пілотному режимі, а також для підвищення безпеки та ефективності. CPS застосовуються для створення медичних пристроїв та систем, які дозволяють моніторити стан пацієнтів у реальному часі, автоматизувати

процеси лікування та діагностики, а також для телемедицини та дистанційного нагляду. CPS допомагають в оптимізації енергетичних мереж та систем, підвищенні енергоефективності, керуванні енергопостачанням, впровадженні розумних систем керування та моніторингу. CPS також використовуються для управління міською інфраструктурою, транспортними системами, енергопостачанням, водопостачанням, відходами, безпекою та багато іншого.

Розробка CPS є важливим напрямом в сучасному інжинірингу, оскільки поєднує в собі компоненти фізичних систем із цифровими технологіями для створення ефективних та інтелектуальних систем. Цей процес включає кілька етапів, які забезпечують успішний розвиток та впровадження CPS.

Загалом можна визначити такі етапи:

1) визначення вимог до системи, де аналізуються потреби користувачів, функціональні вимоги та характеристики системи;

2) проєктування системи, що включає створення архітектури системи, вибір компонентів і технологій, розробку алгоритмів та інтерфейсу;

3) реалізація системи, коли розробники переходять до програмування, збирання та тестування апаратної та програмної частини системи;

4) тестування та валідація системи, де перевіряється відповідність системи вимогам, її функціональність та надійність.

Важливою частиною процесу розробки кіберфізичних систем є постійна оцінка та покращення їх ефективності й безпеки відповідно до змінних умов та вимог користувачів. І. Ш. Невлюдов, В. В. Євсєєв, А. О. Андрусевич, С. С. Максимова зазначають [2], що однією з найбільших проблем у розробці кіберфізичних систем є їх внутрішня складність, неоднорідність і міждисциплінарний характер. Сучасні розподілені CPS об'єднують широкий спектр різнорідних аспектів, таких як фізична динаміка, управління, машинне навчання та обробка помилок [2]. Особливої уваги потребує також питання безпеки кіберфізичних систем. Так І. Фурсов та О. Шматко [3] наводять дані щодо зростання числа атак на кіберфізичні системи, особливо тих, що запущені в критичній інфраструктурі. Науковці зазначають, що великий обсяг інформації, що надходить із тисяч пристроїв, якими обладнані сучасні CPS, і питання захисту таких даних на фізичному та інформаційному рівнях, створюють потребу в нових стратегіях, адаптованих для виявлення сучасних загроз інформаційної безпеки подібних складних систем без перешкод у роботі самої інфраструктури інтелектуальних систем.

Проаналізувавши роботи науковців [1; 2; 3; 4; 5; 6], ми узагальнили небезпеки, що створюють потенційні ризики для безпеки та надійності систем CPS:

- кібератаки, як найбільш розповсюджені загрози, коли зловмисники зламують цифрові компоненти CPS,

щоб завдати шкоди фізичним об'єктам або порушити їх функціональність. Кібератаки набули особливого зростання в період воєнного стану на території нашої країни;

- слабкий захисті мережі та програмного забезпечення CPS може призвести до несанкціонованого доступу, витоку даних або порушення конфіденційності;

- помилки в програмному забезпеченні, апаратні збої або несправності можуть спричинити відмову в роботі фізичних систем, що може призвести до серйозних наслідків, особливо в галузях критичної інфраструктури;

- компрометація, втрата або підробка даних у цифровій частині CPS може призвести до некоректної роботи фізичних процесів або навіть до аварій;

- недостатня інтеграція та взаємодія між цифровими та фізичними компонентами може призвести до нестабільності та невідповідності системи;

- проблеми з безпекою підключених пристроїв. Зростання кількості підключених до мережі пристроїв (IoT) створює нові вектори атак та підвищує загрозу для безпеки кіберфізичних систем.

Для зменшення цих ризиків потрібно впроваджувати ефективні заходи кібербезпеки, ретельно тестувати та валідувати системи, а також постійно вдосконалювати їх заходи захисту від нових загроз.

**Список використаних джерел:**