

URL:https://proceedings.neurips.cc/paper_files/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf

2. Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition URL:<https://arxiv.org/pdf/1409.1556.pdf>

Лунгол Ольга, Габорець Ольга

Донецький державний університет внутрішніх справ

ВИВЧЕННЯ КІБЕРФІЗИЧНИХ СИСТЕМ В ЗАКЛАДАХ ОСВІТИ ЗІ СПЕЦИФІЧНИМИ УМОВАМИ НАВЧАННЯ

Кіберфізичні системи – це інтегровані системи, що об'єднують фізичні об'єкти з комп'ютерною технологією та мережевими зв'язками. Вони реалізують взаємодію між фізичними та цифровими компонентами, щоб сприяти автоматизації, моніторингу, контролю та оптимізації різноманітних систем та процесів. У кіберфізичних системах фізичні об'єкти (такі як механізми, пристрої, датчики) з'єднуються з комп'ютерною програмною частиною та мережевими засобами зв'язку. Це дозволяє системі отримувати в реальному часі інформацію про фізичний світ, а також впливати на нього за допомогою алгоритмів та керуючих сигналів.

Кіберфізичні системи широко застосовуються у таких галузях, як виробництво, транспорт, медицина, енергетика, сільське господарство, правоохоронна діяльність, військова сфера тощо [1 – 3]. Вони дозволяють покращити ефективність, безпеку та ресурсозбереження у ряді технічних систем.

Використання кіберфізичних систем у правоохоронній діяльності надає значний потенціал для підвищення ефективності відповідної галузі. Кіберфізичні системи (КФС) дозволяють правоохоронним органам встановлювати та відстежувати рухи й дії підозрілих осіб або об'єктів за допомогою вбудованих сенсорів, GPS та мережових технологій. КФС можуть бути інтегровані з алгоритмами штучного інтелекту для автоматичного виявлення потенційно небезпечних ситуацій, що дозволяє швидше реагувати та запобігати злочинності. КФС забезпечують та обробляють великі обсяги даних, які можуть бути використані для аналізу та передбачення кримінальної діяльності, що дозволяє правоохоронним органам краще розуміти та відстежувати злочинні тенденції. Такі системи дозволяють виявляти та попереджати кібератаки на інформаційні системи правоохоронних органів, забезпечуючи захист від несанкціонованого доступу та витоку

конфіденційної інформації. КФС можуть бути використані для керування дронами та відеоспостереженням, що дозволяє правоохоронним органам здійснювати нагляд та контроль над великими територіями або небезпечними районами, що особливо актуально в умовах воєнного стану.

Зважаючи на широке коло використання кіберфізичних систем, в тому числі безпосередньо у правоохоронній діяльності, важливого значення набуває вивчення принципів розробки та застосування таких систем майбутніми правоохоронцями для більш компетентного виконання своїх обов'язків. Освіта щодо КФС допоможе майбутнім поліцейським у кращому розумінні принципів безпеки та захисту інформації для запобігання кібератакам, зламам систем та витокам конфіденційної інформації. Розуміння алгоритмів роботи КФС сприятиме покращенню ефективності службової діяльності, таких як моніторинг та відстеження злочинності, аналіз даних та виявлення кримінальних тенденцій, розробки та впровадження превентивних заходів і стратегій захисту.

Отже, вивчення кіберфізичних систем в закладах освіти зі специфічними умовами навчання є важливим фактором забезпечення якісної підготовки сучасних висококваліфікованих фахівців в галузі правоохоронної діяльності. Вивчення КФС допоможе здобувачам освіти засвоїти принципи роботи та застосування сучасних технологій, а також розуміти особливості функціонування цифрового простору. Це сформує у майбутніх поліцейських готовність до викликів сьогодення, що стоять перед сучасною правоохоронною системою.

Список джерел:

1. Mohamed N., Al-Jaroodi J., Jawhar I. Cyber-Physical Systems Forensics: Today and Tomorrow. *Journal of Sensor and Actuator Networks*. 2020. № 9(3). 37. <https://doi.org/10.3390/jsan9030037>
2. Choudhury T. Introduction to Cyber Security and Cyber-Physical Systems. 2021. URL: <http://surl.li/spntx>.
3. Amit K.T., Sreenath N. Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*. Vol. 1. 2021. Pp. 22-33. <https://doi.org/10.1016/j.iotcps.2021.12.002>.