УДК 004.056
**І.В. Ярощук – ст. гр. СБм-61, Ю.Л. Скоренький к.ф.-м.н., доц.**
(Тернопільський національний технічний університет імені Івана Пулюя)

# РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД ДЛЯ РОЗРОБКИ БЕЗПЕЧНИХ КІБЕРФІЗИЧНИХ СИСТЕМ НА БАЗІ ARDUINO

UDC 004.056
**I. Yaroshchuk, Dr. Yu. Skorenkyy**
(Ternopil Ivan Puluj National Technical University)

## RISK-ORIENTED APPROACH FOR DEVELOPING SECURE ARDUINO-BASED CYBERPHYSICAL SYSTEMS

Ключові слова: інформаційна безпека, кіберфізичні системи, оцінка ризиків, Arduino.
Key words: informational security, cyberphysical systems, risk assessment**,** Arduino.

В Україні та світі масово розвиваються системи IoT, з ними розробляється величезна кількість кіберфізичних систем. Під терміном кіберфізичні системи слід розуміти сукупність обчислювальних та фізичних складових, які спроєктовані та взаємодіють між собою як єдина система, що може адаптуватись до змін фізичного середовища [1]. Ці системи проникли майже у всі сфери життєдіяльності людини, де надають нові функціональні можливості, що покращують якість життя та технологічні процеси в різних сферах.

Arduino є однією з найпопулярніших фізично-програмних платформ [1, 2] і являє собою невеликий електронний пристрій на друкованій платі, який дає змогу керувати великою множиною датчиків, електродвигунами, освітленням а також забезпечує можливість передачі та отримання інформації. Платформа Arduino це готовий електронний блок [2, 3] для якого доступне спеціалізоване програмне забезпечення. Мікроконтролери Arduino завдяки своїй доступності, практичності та великій множині сфер застосування можна легко використовувати для розробки КФС.

При розробці кожної системи, в тому числі кіберфізичної, потрібно враховувати всі ризики і загрози, які можуть виникнути після введення системи в експлуатацію. Ризики для безпеки спричинені взаємодією між середовищем та КФС, всередині КФС і між КФС та авторизованими користувачами. Оцінка та управління ризиками зосереджені на виявленні вразливих місць в системі та оцінці можливих збитків.

На основі зробленого аналізу можна стверджувати, що основні ризики для КФС спричинені вразливостями платформи, мережі, програмного та апаратного забезпечення, а також технічними вразливостями та вразливостями управління. Формалізацію якісної оцінки доцільно проводити, спираючись на досвід експертів, тоді як кількісна оцінка має бути побудована на аналізі об’єктивних числових даних.

В доповіді виділено та охарактеризовано методології оцінки ризику для забезпечення безпечної розробки кіберфізичних систем.

**Література.**

1. Alur R. Principles of Cyber-Physical Systems. MIT Press, 2015. - 464 p.
2. Ziemann V. A. Hands-On Course in Sensors Using the Arduino and Raspberry Pi. Boca Raton: CRC Press, 2018. - 258 p.
3. Гаврілов Д. В., Осадчук О. В., Звягін О. С. Основи комп’ютерного проектування та моделювання РЕА. Лабораторний практикум. Частина 1 – Вінниця : ВНТУ, 2015. – 99 с.