УДК 004.056

В.Б. Дудикевич[1], В.М. Максимович[2],
А.Я. Горпенюк[1], Л.Т. Пархуць[1], Г.В. Микитин[1],
Л.В. Мороз[2], С.С. Войтусік[2]
Національний університет "Львівська політехніка"
[1]кафедра захисту інформації,
[2]кафедра безпеки інформаційних технологій

КОНЦЕПЦІЯ ПОБУДОВИ ЗАХИЩЕНИХ КІБЕР-ФІЗИЧНИХ СИСТЕМ

Розроблено концепцію створення багаторівневої комплексної системи безпеки (КСБ) кібер-фізичних систем (КФС), яка спрямована на забезпечення захищеної взаємодії рівнів та компонентів.

The concept of creating a multilevel complex security system (CSS) of cyber-physical systems (CFS) was developed, which aims to ensure a secure interaction of levels and components.

Вступ. Розроблення методологічних засад захисту інформації в кібер-фізичних системах, опрацювання вимірювальної інформації є вагомим у контексті забезпечення безпеки системи "контроль цільових об'єктів – обробка інформації – управління" і дає підстави для ефективної реалізації комплексу наукових завдань, зокрема рамкової програми ЄС "Горизонт – 2020".

Аналіз останніх досліджень та постановка проблеми. Актуальним є розвиток підходів до побудови кібер-фізичних систем, які використовуються у різних предметних сферах. В роботі [1] представлені архітектурні моделі КФС: 1) двокомпонентний взаємозвязок фізичних і кібер технологій, які взаємоміють із людиною, як користувачем, та соціо-техно-економічним середовищем; 2) трикомпонентний взаємозвязок фізичних, синергічних, кібер технологій, які взаємоміють із людиною, як користувачем, та соціо-техно-економічним середовищем. В роботі [2] представлено засади проектування виробничих кібер-фізичних систем на рівнях архітектури: підключення, перетворення, кібер, пізнання, конфігурації. У роботі [3] запропоновано універсальну платформу для побудови прикладних кібер-фізичних систем: об'єкт дослідження та управління; організація вимірювально-обчислювальних процесів; збір, попередня обробка та передавання вимірювальної та службової інформації; організація та здійснення дій управління об'єктом; захищений обмін, опрацювання та зберігання вимірювальної і службової інформації; користувач. **Мета роботи** – створити концепцію побудови КСБ за архітектурою бааторівневих КФС, яка дозволить реалізувати захист інформації у просторі "конфіденційність – цілісність – автентичність".

Методологія побудови захищених кібер-фізичних систем. ***Модель "багаторівнева КФС – багаторівнева КСБ".*** Кібер-фізична система за архітектурою [3] об'єднує кібернетичний та фізичний простори (КП, ФП) шляхом інтеграції обчислювальних та фізичних процесів за допомогою давачів і виконавчих пристроїв. Багаторівнева КФС згідно структури "архітектура – функції – вимоги – застосування": фізичний простір, комунікаційне середовище (КС), кібернетичний простір – контроль, обробка, управління – гарантоздатність, еталонна модель OSI, вимоги до давачів – масштабованість, реконфігурація у контексті багатофункціонального дослідження комплексу факторів впливу на різнорідні об'єкти

предметних сфер. Структура багаторівневої комплексної системи безпеки КФС: комплексні системи безпеки КП, КС, ФП, як підсистем захисту КСБ: управління доступом; ідентифікації та аутентифікації; криптографії; аудиту; забезпечення цілісності, конфіденційності, аутентичності інформації. Система управління комплексною безпекою КФС: модель “плануй – виконуй – перевіряй – дій”; концепція“об’єкт – загроза – захист”. У створенні коиплексної системи безпеки КФС доцільно використовувати: системний підхід – принципи ієрархічності, структуризації, цілісності; синергетичний підхід – властивість емерджентності.

Концепція багаторівневої КСБ кіберфізичної системи. Структура концепції представлена на рис. 1: Згідно концепції “об’єкт – загроза – захист”: *об’єкт* захисту – багаторівнева кібер-фізична система (КП, КС, ФП); *загрози* відповідно для КП, КС, ФП – (показано кривими лініями); *захист* – комплексні системи безпеки для КП, КС, ФП і КФС.

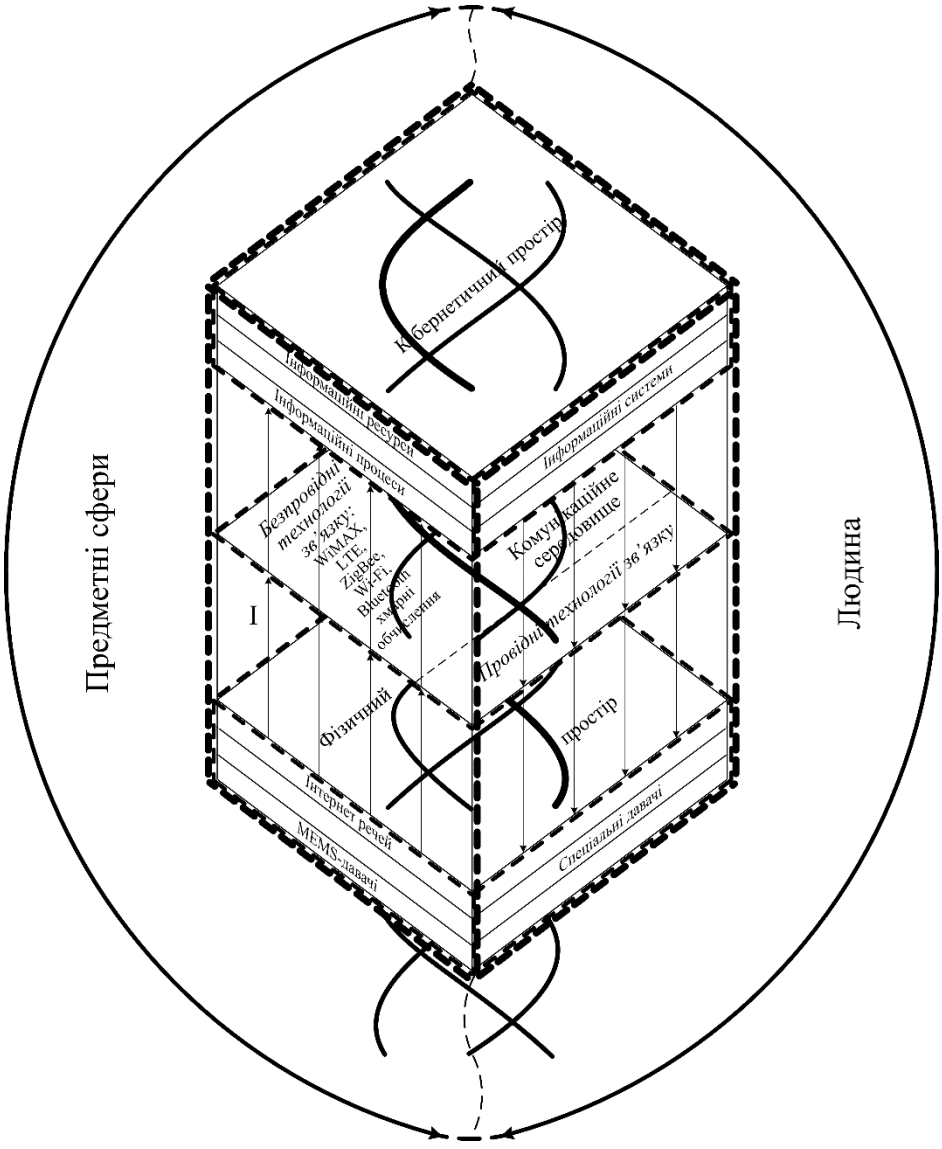

Рис. 1. Структура концепції побудови багаторівневої КСБ кібер-фізичних систем:
I ⟶ – інформація (відбір, управління); ▬ ▬ ▬ – КСБ КП, КС, ФП; ▬▬▬ – КСБ КФС.

Концепція обумовлена структурою: класифікація загроз/атак – формування критеріїв захищеності – створення багаторівневої КСБ КФС – обгрунтування моделі політики безпеки

– вибір методу оцінювання стану захищеності КФС. Класифікація: загроз за ознаками; атак за кінцевим результатом, за способом здійснення; методика класифікації загроз STRIDE за категоріями (підміна обєктів, модифікація даних, відмова від авторства, розголошення інформації, відмова в ослуговуванні, підвищення привілеїв – створення моделі загроз “інформація/КФС – джерела виникнення загроз – способи реалізації загрози”. Критерії захищеності інформації в КФС: архітектура конфіденційності, цілісності, доступності, спостереженості, гарантій. Створення багаторівневої КФС: методичні вказівки щодо розроблення технічного завдання на створення КСБ – обгрунтування вимог до комплексної системи безпеки у сегментах захисту від несанкціонованого доступу та гарантій. Обгрунтування політики безпеки КФС: аналіз моделей та критерії вибору. Оцінювання рівня захищеності КФС: застосування уніфікованих методів забезпечення гарантоздатності.

Висновок. Запропонована концепція побудови багаторівневої КСБ КФС є підставою для реалізації масштабованої та реконфігуровної універсальної платформи у частині методологічних засад захищеного обміну.

Література

Imre Horváth, Bart H. M. Gerritsen. Cyber-physical systems: concepts, technologies and implementation principles // 9th International Symposium on Tools and Methods of Competitive Engineering (TMCE), May 7–11, 2012, Karlsruhe, Germany.

Jay Lee, Behrad Bagheri, Hung-An Kao. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), University of Cincinnati, Cincinnati, OH, United States (Спільний дослідницький центр з інтелектуальних систем технічного обслуговування (IMS), Університет Цинциннаті, Цинциннаті, Огайо, США), 2014.

Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку// Вісник Національного університету "Львівська політехніка". Комп’ютерні системи та мережі. - 2014. - № 806. - С. 154-161.

Наукові результати, подані у цій статті, було отримано в рамках дослідницького проекту ДБ/КІБЕР з реєстраційним номером 0115U000446, 01.01.2015 - 31.12.2017, фінансово підтриманим Міністерством освіти та науки України.