УДК 004.056

В. Б. Дудикевич[1], В. М. Максимович[2], Г. В. Микитин[1]
Національний університет "Львівська політехніка",
[1]кафедра захисту інформації,
[2]кафедра безпеки інформаційних технологій

ПАРАДИГМА ТА КОНЦЕПЦІЯ ПОБУДОВИ БАГАТОРІВНЕВОЇ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ

Розроблено парадигму та концепцію побудови багаторівневої комплексної системи безпеки (КСБ) кіберфізичних систем (КФС), яка орієнтована на розвиток концептуальних засад захищеної взаємодії рівнів та компонентів у просторі "конфіденційність – цілісність – автентичність" відповідно до етапів створення та функціональної реалізації КФС у предметних сферах.

Ключові слова: кіберфізична система, комплексна система безпеки, кібернетичний простір, комінікаційне середовище, фізичний простір, інформація.

The paradigm and concept of cyber-physical systems (CPS) multilevel complex security system (CSS) were developed. They are focused on growth of conceptual principles of secured level interaction and components in the space "confidentiality – integrity – authenticity" according to phases of CPS creation and functional realization in subject spheres.

Key words: cyber-physical system, complex security system, cybernetic space, communication environment, physical space, information.

Вступ

Розроблення підходів, способів і технологій побудови кіберфізичних систем, зокрема у частині взаємодії з сегментами опрацювання та захисту інформації, є актуальним напрямом у контексті вирішення наукових, технічних, соціально-економічних задач головних векторів – національної парадигми сталого розвитку України; воєнної (оборонної) доктрини України. Формування методологічних засад захисту інформації в КФС, опрацювання вимірювальної інформації є вагомим у контексті забезпечення безпеки системи "контроль цільових об'єктів – обробка інформації – управління" і дає підстави для ефективної реалізації комплексу задач за вектором безпеки Стратегії сталого розвитку "Україна – 2020" та створення базового підходу до забезпечення інформаційної безпеки в межах проекту Концепції інформаційної безпеки України у частині забезпечення створення і функціонування системи захисту процесу розвитку інформаційного простору від загроз комунікативного і технологічного характеру.

Аналіз останніх досліджень та публікацій

Кіберфізична система об'єднує кібернетичний та фізичний простори (КП, ФП), інтегруючи обчислювальні та фізичні процеси за допомогою давачів і виконавчих пристроїв. Розвиток КФС розпочато Інститутом стандартів і технологій ((NIST), США) (термін запропоновано *Хелен Джилл, 2006*). Актуальним є розвиток підходів до побудови кіберфізичних систем. У роботі [1] наведено архітектурні моделі КФС: 1) двокомпонентний взаємозв'язок фізичних і кібертехнологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем; 2) трикомпонентний взаємозв'язок фізичних, синергічних кібертехнологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем. Розглянуто принципи реалізації моделей КФС: системних (цілісних) зв'язків; специфікації на основі моделей; розробки на основі платформ; обчислень у режимі реального часу; управління на основі подій; функціональності, орієнтованої на послуги; мінімальної інтрузивності. Розкрито технології реалізації трикомпонентної КФС: кіберкомпонента реалізується як програмні технології, технології передавання і зв'язку, мережеві технології; синергічна реалізується через технології цифрових

мікросхем, сенсорні технології та мережі, мініелектрмеханічні технології; фізична компонента реалізується як технології передових матеріалів, передові енергетичні та роботичні технології. В праці [2] наведено засади проектування виробничих кіберфізичних систем на рівнях архітектури: підключення, перетворення, кіберпізнання, конфігурації. У роботі [3] запропоновано універсальну платформу для побудови прикладних кіберфізичних систем: об'єкт дослідження та управління; організація вимірювально-обчислювальних процесів; збирання, попередня обробка та передавання вимірювальної та службової інформації; організація та управління об'єктом; захищений обмін, опрацювання та зберігання вимірювальної і службової інформації; користувач. Розвиваються дослідження із створення структур захисту інформації в кіберфізичних системах. Наприклад, згідно із стандартом [4] проектують структури "глибокого захисту" мереж прикладних КФС: план безпеки – розподілення мереж – захист периметра мережі – сегментація мережі – підвищення захищеності пристроїв – моніторинг/ оновлення.

Активно обговорюються напрямки застосування КФС у контексті: 1) створення інтелектуального виробництва, інтелектуального енергопостачання, інтелектуальних споруд, інтелектуального транспорту, інтелектуальних систем оборони; 2) формування Інтернет речей (поняття запропонував *Кевін Ештон, 1999*) як мережі фізичних об'єктів з вбудованими давачами для реєстрації та передавання даних про стан різнорідних об'єктів, середовища та структури взаємодії "об'єкт – середовище". Перспектива сьогодні за: Інтернет всього (поняття запропонував *Дейв Еванс, 2012*) як комплексної системи – людей, процесів, даних, технічних пристроїв з метою формування необхідного та ефективного інформаційного рівня мережевих з'єднань; промисловим Інтернетом (поняття введено *альянсом Industrial Internet Consortium: CISCO, IBM, Intel*) як складною самоконфігурованою адаптивною системою мереж давачів та розумних об'єктів, призначення яких полягає у з'єднанні усіх речей, зокрема побутових і промислових об'єктів. В сучасній інфраструктурі суспільства актуальним стає проектування Інтернет чого завгодно як єдиної програмної екосистеми, що підтримує комплекс показів: усіх давачів, системних станів, експлуатаційних умов, контекстів даних. Ефективне функціонування інтелектуальних об'єктів у предметних сферах забезпечують КФС, структуровані Інтернет речей на рівні комінікаційного середовища (КС). Інтернет речей як мережа мереж структурується рівнями: індивідуальних мереж; з'єднаних мереж, що забезпечують зв'язок між індивідуальними мережами; мережі зв'язку з системами безпеки та керування. Функціональність Інтернет речей: масштабованість, доступність, керованість, управління даними, безпека, зручність користування. Відповідно актуальною проблемою у галузі інформаційної безпеки є розроблення стратегії забезпечення захищеного функціонування усіх рівнів, компонент та взаємозв'язків прикладних КФС у площинах кібернетичного і фізичного просторів та комунікаційного середовища.

Постановка задачі. Рівень безпеки енергетичних та оборонних об'єктів, екологічних систем середовища в глобальному інформаційному просторі зумовлюється проектуванням і впровадженням захищених багаторівневих кіберфізичних систем. Системний підхід до побудови багаторівневої КСБ КФС уможливить захист інформації на рівні взаємозв'язку – взаємодії – взаємодоповнення структур: багаторівнева КФС – багаторівневий захист; багатофункціональність КФС – захищений контроль, обробка/обмін, управління; гарантоздатність КФС – функціональна та інформаційна безпека та реалізація синергетичного ефекту багаторівневого захисту, розглядаючи КФС як багаторівневу структуру, що має властивості масштабованості та реконфігурації відповідно до функціональних задач у предметних сферах. ***Мета роботи*** – побудова нової парадигми розроблення захищених КФС, ядром якої є концепція створення КСБ та моделі концепції управління інформаційною безпекою КФС з метою забезпечення захищеного обміну інформації у просторі: конфіденційність – цілісність – автентичність.

Парадигма та концепція побудови багаторівневої комплексної системи безпеки кіберфізичних систем

Для забезпечення цілісності, конфіденційності та автентичності інформації в КФС, розвитку технічного і криптографічного захисту компонент КФС та їх інформаційної взаємодії, безпечного управління доступом до компонентів КФС розглянемо парадигму та концепцію побудови

багаторівневої КСБ багаторівневої КФС, яка дасть змогу реалізувати захищений обмін, опрацювання, зберігання вимірювальної та службової інформації.

Парадигма "багаторівнева КФС – багаторівнева КСБ". Багаторівнева КФС згідно із структурою "архітектура – функції – вимоги – застосування": фізичний простір, комунікаційне середовище, кібернетичний простір – контроль, обробка, управління – гарантоздатність, еталонна модель OSI, прецизійність давачів – масштабованість, реконфігурація у контексті багатофункціонального дослідження комплексу факторів впливу на різнорідні об'єкти предметних сфер. Структуру парадигми багаторівневої КСБ КФС наведено на рис. 1. За структурою парадигми, комплексні системи безпеки ФП, КС, КП як підсистеми захисту КФС передбачають: управління доступом; ідентифікацію та аутентифікацію; криптографію; аудит; забезпечення цілісності, конфіденційності, аутентичності інформації. Система управління комплексною безпекою КФС грунтується на моделі "плануй – виконуй – перевіряй – дій" та концепції"об'єкт – загроза – захист".

Методологічні піходи до створення КСБ КФС. Методологія створення КСБ КФС охоплює: системний підхід – принципи ієрархічності, структуризації, цілісності, які дають підстави для створення комплексної системи безпеки КФС у сегменті оптимального поєднання: нормативно-методичного, організаційного, інформаційного, технічного (апаратного), програмного забезпечення на етапах життєвого циклу автоматизованих систем; синергетичний підхід – властивість емерджентності, що проявляє одну з граней цілісності захисту інформації в КФС та припускає наявність властивостей, що притаманні комплексній системі безпеки КФС загалом, але не властиві її окремим елементам – комплексним системам безпеки КП, КС, ФП.

Рис. 1. Структура парадигми побудови багаторівневої КСБ кіберфізичних систем

Концепцію створення багаторівневої КСБ кіберфізичної системи наведено на рис. 2. Концепція зумовлена структурою: класифікація загроз/атак – формування критеріїв захищеності – створення багаторівневої КСБ КФС – обгрунтування моделі політики безпеки – вибір методу оцінювання стану захищеності КФС [5, 6]. Класифікація загроз/ атак: загроз за ознаками; атак за кінцевим результатом, за способом здійснення; методика класифікації загроз STRIDE за категоріями (підміна об'єктів, модифікація даних, відмова від авторства, розголошення інформації,

відмова в обслуговуванні, підвищення привілеїв) – створення моделі загроз “інформація/КФС – джерела виникнення загроз – способи реалізації загроз”. 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 КСБ у сегментах захисту від НСД та гарантій. Обгрунтування політики безпеки КФС: аналіз моделей та критерії вибору. Оцінювання рівня захищеності КФС: застосування уніфікованих методів забезпечення гарантоздатності [7].

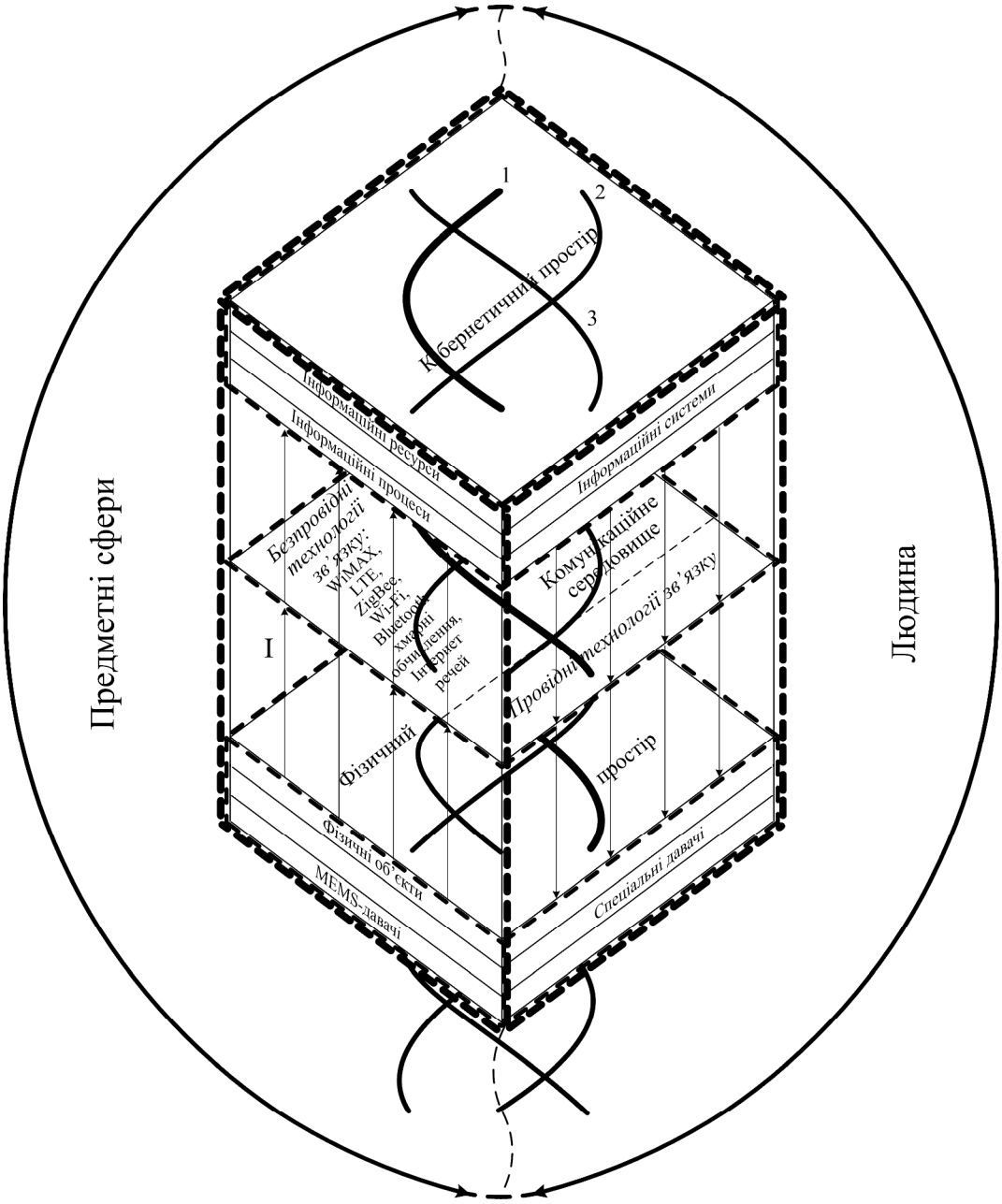

Рис. 2. Структура концепції побудови багаторівневої КСБ кіберфізичних систем:
I ⟶ – інформація (відбір, управління); ▬ ▬ ▬ – КСБ КП, КС, ФП; ▬▬▬ – КСБ КФС;
1.2.3 – загрози відповідно для КП, КС, ФП

Комплексні системи безпеки КП формуються на основі концепції “об’єкт – загроза – захист” відповідно до сегментів: інформаційні ресурси – бази даних, бази знань, бази моделей, масиви інформації, сховища даних; автоматизовані системи – модель гарантоздатності, модель багаторівневого і багатоланкового захисту; інформаційні процеси – фази, операцій, обробка.

Комплексні системи безпеки КС створюються на основі концепції “об’єкт – загроза – захист” відповідно до сегментів: безпровідні технології зв’язку – ZigBee, Wi-Fi, Bluetooth, WiMAX, LTE, хмарні обчислення, Інтернет речей: модель взаємодії відкритих систем (OSI); структура “інформаційна безпека – цілісність даних – надійність – рівень обслуговування – утилізація інформації”; провідні технології зв’язку – системи волоконно-оптичні, системи коаксіальні (мідь): загальні технічні умови та вимоги.

Коиплексні системи безпеки ФП розробляються на основі концепції “об’єкт – загроза – захист” відповідно до сегментів: давачі, вбудовані у різнорідні фізичні об’єкти; спеціальні давачі, вбудовані у пристрої (електронна та аерокосмічна розвідка, дистанційний моніторинг параметрів екосистем планети, спостереження стану надзвичайних ситуацій, виявлення рухомих і нерухомих об’єктів у воєнних ситуаціях; пошук об’єктів); MEMS-давачі (широкий спектр застосування, зокрема в системах безпеки) – вимоги до параметрів давачів з метою забезпечення точності відбору, реєстрації та передавання інформації в КП, опрацювання вимірювальних даних системами та передавання інформації на управління інтелектуальними об’єктами фізичного простору.

Концепція управління КСБ кіберфізичних систем ґрунтується на розробленні методології: аналіз моделей і методів – обгрунтування їх застосування у системі управління інформаційною безпекою багаторівневої КФС – коригувальна дія у контексті модифікації структури концепції КСБ кіберфізичних систем [8].

Висновок

Створена парадигма та концепція побудови КСБ кіберфізичних систем спрямовані на забезпечення системного та синергетичного ефекту захисту інформації відповідно до архітектури: кібернетичний простір – комунікаційне середовище – фізичний простір. Універсальна структура концепції трансформується у різні предметні сфери, модифікується на рівні “багаторівнева КФС – багаторівневий захист” та забезпечує конфіденційність, цілісність, автентичність інформації згідно системи нормативного забезпечення.

1. 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. 2. 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, 2014. 3. Мельник А. О. Кібер-фізичні системи: проблеми створення та напрями розвитку// Вісник НУ “Львівська політехніка”. Комп’ютерні системи та мережі. – 2014. – № 806. – С. 154 – 161. 4. National Institute of Standards and Technology Special Publication 800-82. – NIST SP 800-53 – 2011. – 155 p. 5. Space product assurance. Methods and techniques to support the assessment of software dependability and safety. – ECSS-Q-80-03, 2006. – 122 p. 6. Information processing systems. Open Systems Interconnection. Basic Reference Model – Part 2: Security Architecture, – ISO 7498-2:1989. – 32 p. 7. National Institute of Standards and Technology Special Publication 800-53. – NIST SP 800-53, Rev. 4, 2013. – 462 p. 8. Information technology. Telecommunications and information exchange between systems. Security framework for ubiquitous sensor networks: ISO/IEC 29180:2012. – 34 p.