CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2020.8.1.218013
УДК 004.056.53::[007.51+62-529+64.011.34]

ЮЛІЯ КОЖЕДУБ,
ЮЛІЯ КРАМСЬКА,
ВІРА ГИРДА

АНАЛІЗ ВПЛИВУ ЛЮДСЬКОГО ФАКТОРУ НА КІБЕРФІЗИЧНУ СИСТЕМУ

Досліджено питання стрімкого застосування технологій Четвертої промислової революції для різних сторін життя людства, що узагальнює різноманітні технічні засоби та інформаційні технології завдяки імплементації кіберфізичних систем, кіберфізичних виробничих систем та Інтернету речей у виробництво товарів та сферу надання послуг. Проаналізовано широке поширення кіберфізичних систем як нового механізму та способу досягнення нового, більш високого рівня життя людей. Кіберфізичні системи збирають, зберігають й аналізують дані, отримані від різноманітних датчиків. Це потрібно для надання узагальненої інформації та подальшого використовування її для об'єднання віртуального та фізичного середовищ. Метою такого об'єднання є створення мережевого середовища в якому інтелектуальні об'єкти взаємодіють один з одним. Наразі кіберфізичні системи забезпечують інтеграцію обчислювальних засобів у фізичні процеси, а в майбутньому такі системи передбачатимуть упровадження в процеси управління елементів штучного інтелекту. Це необхідно тому, що людина вже не здатна забезпечувати ефективне управління у рамках наявних автоматизованих систем надзвичайно складними виробничими, технологічними і соціальними процесами. Тому акцентовано увагу на ризиках кіберфізичних систем та показано важливість поводження з ними. Наведено їхню класифікацію з урахуванням впливу застосування технологій Четвертої промислової революції з використанням кіберфізичних систем. Ця класифікація охоплює складові, що відображають кожен компонент нової інноваційної концепції – Четвертої промислової революції. Досліджено основні причини помилок функціонування систем "людина-машина" стосовно упередженості людини. З'ясовано, що кіберфізичні системи охоплюють взаємозалежні аналогові, цифрові, фізичні та людські компоненти, розроблені для функціонування за допомогою інтегрованих фізичних пристроїв та логічних елементів. Наведено визначення терміну "когнітивне упередження". Сформульовано, що кіберфізичні системи мають дев'ять аспектів, які мають назву "кластери проблем". Переваги та недоліки від застосування новітніх технологій Четвертої промислової революції залежатимуть від необхідності оцінювання балансу "користь-безпека" для еволюційного процесу загалом і конкретної людини, зокрема.

Ключові слова: Четверта промислова революція, кіберфізична система, система "людина-машина", людський фактор, упередження, ризики, кіберзахист.

Постановка проблеми. Четверта промислова революція, більш відома як "Промисловість 4.0" (анг. Industry 4.0, нім. Industrie 4.0), отримала свою назву від ініціативи 2011 року, яку очолювали бізнесмени, політики і вчені Німеччини, що визначили її як засіб підвищення конкурентоспроможності обробної промисловості своєї країни через посилену інтеграцію кіберфізичних систем (англ. Cyber-Physical Systems, CPS; укр. акронім КФС), у виробничі процеси [1], [2].

Четвертою промисловою революцією встановлено поєднання двох середовищ: виробничого і мережевого шляхом використання КФС, кіберфізичних виробничих систем (англ. "Cyber-Physical Production Systems", CPPS; укр. акронім КФВС) і Інтернету речей (англ. "Internet of

© Ю. Кожедуб, Ю. Крамська, В. Гирда, 2020

Things", IoT; укр. акронім ІР). Сьогодні ця революція характеризується соціальними медіа та комунікаціями Машина-до-Машини (M2M). За допомогою смарт-продуктів і автономних транспортних систем у подальшому це призведе до створення повністю інтегрованих заводів і концепцій Plug & Produce, тобто шляхом з'єднання машин, деталей, пристроїв і систем через інтелектуальні мережі будуть створюватись ланцюжки, елементи яких можуть керувати один одним автономно. Наступним кроком буде перехід від традиційної п'ятирівневої піраміди автоматизації (що складається з CNC – Computer Numerical Control, PLC – Programmable Logic Controller, SCADA – Supervisory Control and Data Acquisition, MES – Manufacturing Execution System і ERP – Enterprise Resource Planning) до надзвичайно гнучких в підключенні інтелектуальних фабрик (iFactories) на основі Хмари [1]. Потім мережеві машини і виробничі системи зможуть самостійно обмінюватися інформацією й обробляти її для управління промисловими виробничими процесами.

Передбачається, що результатом упровадження Четвертої промислової революції буде створення заводів, які працюють як одна складна машина, а окремі автоматизовані виробничі пристрої будуть підключені як частина повного виробничого процесу. Цей процес використовуватиме підключення КФС (КФВС, датчики, приводи і машини в режимі реального часу), що працюють разом з автоматизованим процесом, який контролює забезпечення і переміщення матеріалів. Нарешті, підключення iFactories до комп'ютерних програм проектування дасть змогу процесу виробництва змінитися в міру появи нових продуктів [1].

Четверта промислова революція покладається на складне програмне забезпечення (ПЗ) і на машини, що взаємодіють один з одним для оптимізації виробництва. Комп'ютеризація виробництва, високий рівень взаємозв'язку, розумні фабрики і зв'язок між обладнанням створюють нову епоху автоматизації, технологій виробництва і розвитку логістики [1]. Є два основних елементи, що дають змогу використовувати переваги Четвертої промислової революції в широкому діапазоні застосунків: M2M в поєднанні з ІР. Зв'язок M2M використовується для автоматичної передачі та вимірювання даних між механічними чи електронними пристроями. Це потрібно для створення інтелектуальної мережі об'єктів і незалежного управління процесами, що є новим аспектом виробничих процесів. Це стане дуже популярним серед користувачів у багатьох галузях, оскільки вони даватимуть змогу отримувати більше цінної інформації з пристроїв, машин і відповідних процесів, таких як: поточний статус, діагностика, параметри процесу.

Сьогоднішні реалії такі, що пристрої, системи і машини будуть підключатись один до одного через наявні в мережі "точки даних", апаратура та пристрої будуть зберігати все більше даних для створення "об'єкта даних" в мережі, який з часом буде зростати до кіберзасноваої ідентичності або "кібероб'єкта".

Програмні послуги будуть все більш доступні для підключення кібероб'єктів до КФС з метою оптимізації процесів. Прикладом є оптимізація потоку трафіку шляхом підключення кібероб'єктів: транспортних засобів і систем світлофорів до КФС, яка потім оптимізує потік трафіку у мегаполісах [1].

Аналіз останніх досліджень і публікацій. Дослідження КФС розпочато в Національному інституті стандартів і технологій (англ. National Institute of Standards and Technology, NIST) Міністерства торгівлі США. Термін запропонувала Хелен Джилл у 2006 р. На сьогодні вельми актуальним є розвиток підходів до побудови КФС. У [3] наведено архітектурні моделі КФС:

1) двокомпонентний взаємозв'язок фізичних і кібернетичних технологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем;

2) трикомпонентний взаємозв'язок фізичних, синергічних, кібернетичних технологій, які взаємодіють із людиною як користувачем та соціотехноекономічним середовищем.

Зазначені моделі КФС мають такі принципи реалізації: наявність системних (цілісних) зв'язків; специфікації на основі моделей; розроблення на основі платформ; обчислення у режимі реального часу; управління на основі подій; функціональність, орієнтована на послуги; мінімальна інтрузивність.

Як зазначено в [4], технології реалізації трикомпонентної КФС є такими: кіберкомпонента – як програмні технології, технології передавання і зв'язку, мережеві технології; синергічна – через технології цифрових мікросхем, сенсорні технології та мережі, міні-електромеханічні технології; фізична – як технології передових матеріалів, передові енергетичні та роботизовані технології.

У [5] визначено сегменти забезпечення безпеки КФС, а саме: виявлення атак, моделювання атак, оцінювання та контроль рівня захищеності. Крім того сформовано напрями досліджень безпеки КФС, серед яких: оцінювання ризиків, стратегії контратак, тестування та перевірка.

У [6] висвітлює проблеми створення та напрями розвитку КФС. Дослідження щодо ПЗ КФС описано в [7]. У [8] показано напрям і етапи розроблення комплексної системи безпеки КФС, заснованої на отриманні інформації з датчиків в системах, які використовують сучасні технології бездротового доступу в Інтернет, що найбільш динамічно зараз розвиваються. Важливість застосування КФС як інноваційної складової майбутнього розвитку економіки (промисловості і сфери надання послуг) відображено в [9].

Підсумковий аналіз наукових доробок показує, що зазначені роботи зосереджені в технічному спрямуванні проблеми застосування КФС. Однак, що є не менш важливим, потрібно проаналізувати роль, місце і значення людини як елемента кіберфізичних систем, так і відповідність КФС щодо заходів кіберзахисту.

Метою статті є дослідження питання стрімкого застосування технологій Четвертої промислової революції для різних сторін життя людства. Аналіз широкого поширення кіберфізичних систем як механізму та способу досягнення нового рівня життя людей. Встановлення місця і ролі людського фактору в КФС для чого проаналізувати компоненти КФС. З'ясування переваг та недоліків новітніх технологій щодо необхідності балансу "користь-безпека" для науково-технічного прогресу і конкретної людини загалом.

Виклад основного матеріалу дослідження. Поширення новітніх технологій Четвертої промислової революції може зумовити величезні зміни у повсякденному житті, надавши звичайним користувачам абсолютно новий рівень комфорту життя. Якщо елементи такої системи не будуть належним чином захищені від несанкціонованого втручання, то замість користі вони принесуть шкоду, надавши порушникам кібербезпеки можливість вчинити кіберзлочин, скориставшись уразливостями через нехтування питаннями безпеки. Це є ймовірним, тому що побутові прилади з вбудованими комп'ютерами зберігають дуже багато інформації про свого власника, зокрема можуть знати його точне місцезнаходження, різноманіття його уподобання і це є чинником, що дещо сповільнює впровадження інтелектуальних систем у повсякденне життя мільйонів людей. Із посиленням ролі таких пристроїв в житті людей буде збільшуватись уразливість даних, навіть найнезначніших на перший погляд. Необхідно оцінювати будь-який витік інформації, так як накопичення й аналіз її складових може представляти небезпеку для приватного життя людей. Все це зумовлює підвищений інтерес до проблеми кібербезпеки [10].

Ризики Промисловості 4.0 можна поділити на [10]:

- ультра нові, що виникнуть лише під час впровадження концепції промислового виробництва у реальне життя, і які взагалі не притаманні нинішній економіці;
- нові ризики, що лише почали виникати на теперішньому етапі розвитку світової економіки: ризики адитивного виробництва, ризики кібербезпеки;
- традиційні (або класичні) ризики, які були, є та будуть властиві розвитку світової економіки та суспільства: інвестиційні ризики, ризики інноваційної діяльності, ризики промислового шпигунства та конкурентної розвідки, адміністративно-законодавчі ризики, ризики управління підприємством, екологічні ризики, ризики ресурсного забезпечення.

Також ризики Промисловості 4.0 можна класифікувати за "центрами" їх виникнення [10]:

- соціальні ризики, пов'язані насамперед зі змінами зайнятості населення у виробництві, його соціальними гарантіями;

– ризики інноваційних засобів та технологій, пов'язані з результатами науково-технічного прогресу;

– економічні ризики, пов'язані з економічними результатами діяльності інноваційних підприємств;

– адміністративно-законодавчі ризики;

– екологічні ризики.

Кожну з зазначених складових ризиків потрібно ідентифікувати, проаналізувати, зіставити й обробити.

Ризики КФС, що пов'язані з різними небажаними ситуаціями у роботі компонентів цих систем, є такими: звичайні фізичні несправності механізмів устаткування; збої в управлінні кібернетичними компонентами фізичних процесів; некоректне переналаштування виробничих процесів; помилки у виборі комплектуючих, які необхідні для виробництва продукції; вибір неправильної програми виробництва продукції; помилки, які можуть статись на різних ділянках виробництва продукції (некоректна обробка інформації, неправильне компонування комплектуючих тощо); моральне "старіння" устаткування та його вузлів [10].

Створення реальних КФС має таке підґрунтя: по-перше, зростання кількості пристроїв із вбудованими мікропроцесорами і засобами зберігання даних; по-друге, інтеграція Інтернету, технічних систем і послуг, об'єднаних у одну загальну складну організаційно-технічну систему, яка утворює "розумне середовище існування" для людей (англ. "Smart Building Environment"). Вже сьогодні є надвеликі системи автоматизованого технологічного управління енергопостачанням цілих континентів, наприклад [11], північноамериканського континенту, залізничними комунікаціями, авіалініями тощо. КФС – це не просто система, що передбачає інтеграцію обчислювальних засобів у фізичні процеси, а система, яка передбачає впровадження в процеси управління елементів штучного інтелекту. Це необхідно тому що людина вже не здатна забезпечувати ефективне управління у рамках наявних автоматизованих систем надзвичайно складними виробничими, технологічними і соціальними процесами.

Поки що не вдалось створити обчислювальні системи, які б могли мислити як людина і одночасно використовувати усі переваги, що має техніка. Просування у сторону вирішення складної проблеми відбувається поступово і малими кроками. Вже сьогодні є достатньо складні системи, що забезпечують управління надзвичайно складними процесами і використовують при цьому такі сучасні складні інформаційні технології як: бази і банки даних, системи підтримки прийняття рішень, бази знань і експертні системи [11]. Створення систем, що будуть здатні забезпечити захист від загроз нового типу, потребує системного аналізу й оцінки загроз, а також відповідних показників безпеки. Сьогодні КФС – це, здебільшого, надвеликі автоматизовані системи управління, фізичною основою яких є надзвичайно розподілені і надзвичайно складні обчислювальні системи, але поки що вони залишаються лише автоматизованими системами. Наступним кроком має бути розроблення систем підтримки прийняття рішень і експертних систем для вирішення широкого кола задач у різноманітних галузях людської діяльності, із застосуванням штучного інтелекту. Проте, людина поки що залишається головною складовою систем управління [12].

КФС складаються з цифрових, аналогових, фізичних та людських компонентів, розроблених для функціонування за допомогою інтегрованої фізичних пристроїв та логічних елементів, що взаємодіють один з одним (див. рис. 1 [13]).

Рамкова концепція КФС (англ. "CPS Framework") забезпечує організоване представлення методології аналізу КФС, засновану на основних її аспектах: грані – це режими інженерного процесу системи, та дев'ять аспектів, – це так звані кластери проблем (див. рис. 2).

Застосування та переваги КФС мають еволюційний і всепоглинальний характер – це важливо, оскільки їх застосовують у нових розумних автомобілях, будинках, роботах,

безпілотних транспортних засобах, медичних приладах (на рис. 2 їх позначено як домени, інакше кажучи – сфери застосування). Функціонування КФС залежатиме не лише від зазначених властивостей й аспектів кожного з компонентів, а ще і від управління ризиками, що разом впливатимуть на надійність, оскільки "система робить те, що потрібно, незважаючи на … помилки користувачів та операторів…" [14].

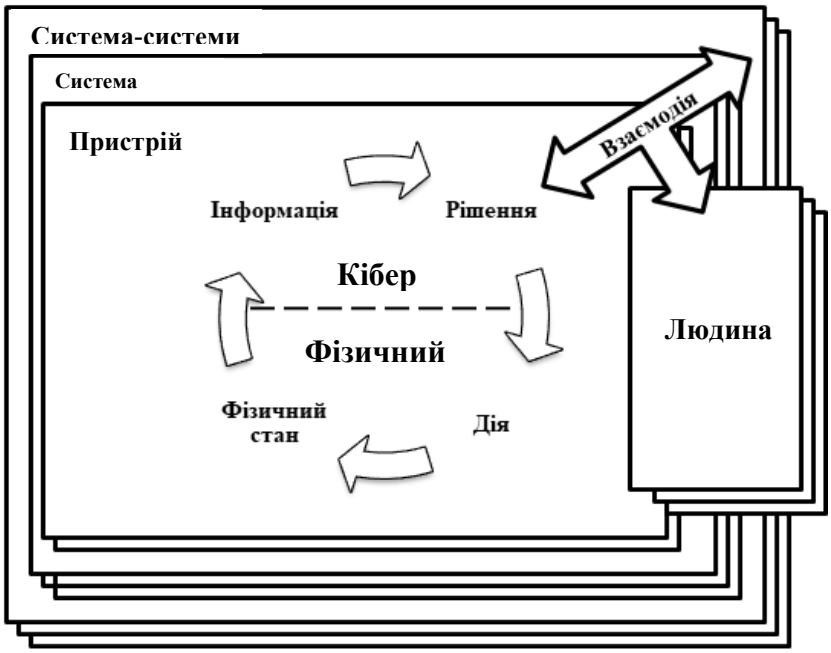

Рисунок 1 – Модель концепції КФС

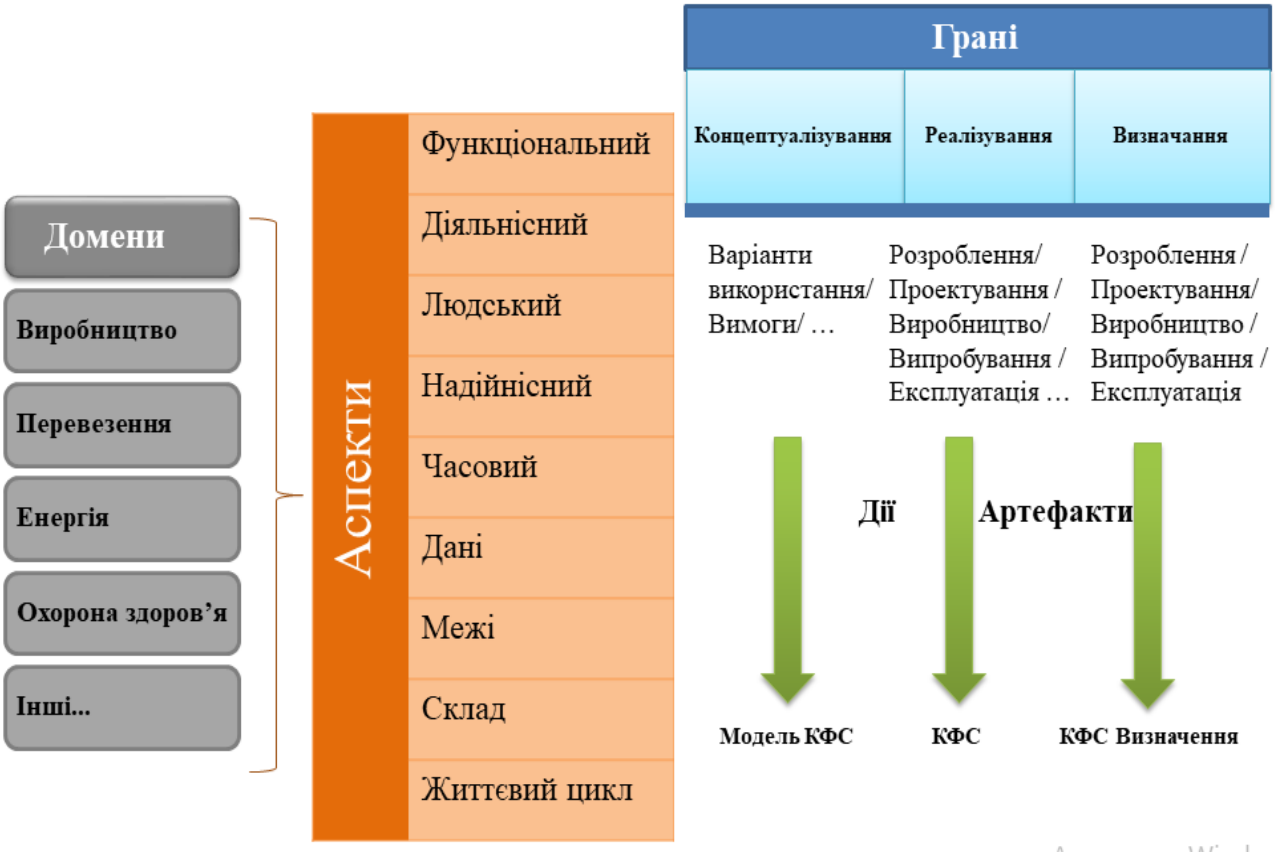

Рисунок 2 – Рамкова концепція КФС

Концепція Четвертої промислової революції наголошує, що поява КФС стосується не лише технічних засобів, а й суспільства у цілому [15]. Під час їх створення доречно зважати на соціокультурні аспекти проблеми автоматизації і роботизації з урахуванням усіх сторін розвитку суспільства.

Людський чинник є невід'ємною складовою КФС, адже людина є рушієм і творцем систем, об'єктом дії. Здебільшого людина стає причиною збоїв і помилок функціонування систем. Людині складно підтримувати високий рівень працездатності, інколи низька швидкість прийняття рішень може призвести до незворотних наслідків, особливо в аварійних ситуаціях.

Наразі провадяться сучасні розробки щодо заміни людей машинами, роботами, застосування автоматизації і роботизації для все ширших сфер діяльності (виробництва, побуту). Звичайно, складнощі можуть виникнути через процеси адаптації поведінкових факторів, що можуть впливати на сферу виробництва. Дослідження системи "машина-людина" має враховувати ефективність роботи оператора (людини), адже функціонування всієї системи в цілому, залежить від раціонального розподілу функцій між людиною і машиною, що виходить з їх переваг і обмежень. Те, що робить людину людиною – якості, що притаманні їй, порівняно з машинами, насамперед це емпатія, а також чуттєвість, емоційність, може шкодити функціонуванню технічних систем. Помилки людини в системі "машина-людина" спричинені станом, властивим людині, що має назву "упередження". Упередження надзвичайно поширені, понад усе вони характерні для тих сфер людської діяльності, які пов'язані з процесами, предметами чи обставинами, про яких немає (або в принципі не може бути) достатньо повної інформації. Також там, де, на перше місце ставиться точність, логічність, адекватність та обґрунтованість (наприклад, в науці), є велика кількість упереджень. Деякі упередження мають ряд когнітивних ("холодних") або мотиваційних ("гарячих") пояснень, досить часто обидва ефекти можуть бути наявними одночасно [16] - [17]. Складність функціонування КФС пов'язана з унікальними елементами та властивостями, спричинено впливом людського фактору, що, в свою чергу привносить наповнення контексту для управління ризиками. Наступне покоління КФС повинно враховувати ризик-орієнтований підхід, який підтримуватиме розвиток систем, стійких за своєю природою. Майбутні покоління КФС повинні мати здатність не лише виявляти загрози, але також повинні мати спроможність зіставляти ці загрози з їх впливом на функціонування системи.

Когнітивне упередження ("когнітивна ілюзія" або "когнітивне спотворення", англ. "Cognitive bias") – відхилення у судженнях, яке супроводжується можливою нелогічністю висновків про інших людей і ситуації [18]. Людина створює свою "суб'єктивну соціальну реальність" на основі власного сприйняття зовнішнього світу. Побудована індивідом соціальна реальність може диктувати його поведінку, що призводить до спотворення сприйняття, неточного судження, нелогічної інтерпретації або "ірраціональності".

Деякі упередження, імовірно, адаптивні. Когнітивні упередження можуть зумовити більш ефективні дії у деяких ситуаціях. Окрім того, когнітивні упередження дають змогу швидше приймати рішення, коли швидкість реакції цінніша за точність. Інші когнітивні упередження є наслідком обмежень людських можливостей щодо оброблення даних чи результатом відсутності відповідних психічних механізмів (обмежена раціональність) [16]. Є набір теорій, що описують модель свідомості з поділом на швидке "інтуїтивне" мислення та усвідомлене, спрямоване на прийняття рішень. Ці системи зазвичай називають експліцитною й імпліцитною, або Системою 1 і Системою 2 [16].

Система 1 – швидка: несвідоме прийняття рішень; відчуття, інтуїція, наміри, почуття; обробляє один потік інформації; не включає логіку і статистику; схильна до всіх упереджень відразу.

Система 2 – повільна: усвідомлене і "повільне" прийняття рішень; перетворює відчуття й інтуїції в переконання; стежить за поведінкою; відносно багатопотокова робота; робить цілеспрямований вибір і дії; вважає себе головною.

Упередження – це вплив людського фактору в системі “людина-машина”. Не можна повністю виключити “похибки”, особливо в стресових, незвичних або в ситуаціях, що стрімко розвиваються. На практиці є конкретні прийоми, які допомагають обходити упередження і зменшити їх вплив на процес і результат роботи, але це складне завдання і навіть знаючи про упередження, люди все одно схильні до нього [19].

Майбутні покоління КФС повинні вирішувати складні поточні проблеми. По-перше, наявні середовища автоматизації є результатом органічного взаємозв’язку КФС, а тому постає проблема неможливості передбачити, визнати та запобігти появі несправностей. По-друге, значна людська помилка може бути як результат надлишку даних, так і трапитись через їхню недостатність, а це є на сьогодні актуальним завданням.

КФС проектують так, щоб мати декілька цілей для досягнення ефективності: ідентифікація, ранжування, встановлення пріоритетності. На противагу цьому людина здатна ситуативно визначати те, що є важливим на даний момент часу. А тому цілі, закладені під час створення системи, можуть призвести до небажаної реакції з боку діяльності людини.

Для запобігання появі проблем (зменшення ризиків) наведемо шляхи їхнього подолання, що потребують цілісного й контрольованого підходу до розуміння багатопрофільного характеру цих питань, пов’язаних з людським фактором КФС [19]:

1. Термінове адаптування до поточних (навколишніх) умов.

1.1. Досяжна ієрархія з напівавтономними рівнями: здатність мати великі масштаби, інтегровані методи наглядового контролю, що реалізують унікальні способи виявлення деградації.

1.2. Складні взаємозв’язки та затримка в часі: широко розподілені елементи КФС, організовані для запобігання дестабілізації її керованості.

2. Проблеми взаємодії машин з людьми.

2.1. Прогнозування працездатності людини: люди мають значні можливості, їх професіоналізм засновано на основі досвіду, але вони не завжди працюють на одному рівні ефективності на противагу машинам.

2.2. Кіберінформованість та розумний противник: здатність розпізнавати та пом’якшувати кібератаки, що є необхідним для забезпечення цілісності КФС.

3. Конфлікти цілей.

3.1. Потенційно суперечливі цілі та хибне розуміння чинників, що впливають на: стабільність, безпеку, ефективність й інші чинники стосовно загальних критеріїв функціонування КФС.

3.2 Відсутність поінформованості державних органів влади: неопрацьовані дані повинні бути переведені в повноцінну інформацію про стан процесу та параметри (характеристики) компонентів (елементів) КФС.

У кількох секторах КФС (включаючи, але не обмежуючись ними, транспорт і реагування на надзвичайні ситуації), область використання динамічна: люди та/чи машини змінюються (наприклад, стан здоров’я та/чи технічний стан, відповідно). Динамічність конфігурації КФС збільшується через те, що вузли або періодично недоступні, або можуть змінити середовище (та супутні вимоги забезпечення безпеки) залежно від завдання, яке виконує КФС. І, головне, змінювана протягом тривалого часу працездатність людей, – це є вагомий доданок до рівня динамічності і впливатиме на функціонування КФС з високим ступенем ймовірності.

Особливі характеристики для різних сфер застосування повинні враховуватись під час розробки та створення безпечних КФС. Надійні архітектури їх повинні базуватись на детальному розумінні фізичних властивостей та наявних обмеженнях. Нижче наведено перелік загроз для систем безпеки КФС [19]:

1. Загрози стійкості

1.1. Не можна знати всіх векторів загроз, а тому розроблення КФС має містити різноманітні методи отримання та збереження даних й адаптації алгоритмів конфігурації щодо перетворення відповіді КФС для реагування на зміни за потребою.

1.2. Кіберзагрози мають адаптивний характер та є “розумними”, ось тому вкрай необхідним є постійний розвиток методології прогнозування характеру потенційних загроз, їхні цілі та вплив на кожну компоненту КФС.

1.3. Складно прогнозувати реакцію КФС через поєднаних технологій і взаємодію між людьми (здатність людей приймати хибні рішення та вплив фальсифікованих показників). Треба також звернути увагу на те, що людина, може бути не здатною достатньо своєчасно зреагувати на деякі загрози, але люди повинні бути обізнані про поточний стан функціонування КФС.

1.4. Поширення цифрових технологій є глобальним, складним процесом і не підпадає під будь-який контроль однієї організації. У кіберзлочинців може бути багато можливостей обійти систему безпеки КФС.

1.5. Підвищена складність проектування й створення КФС має забезпечувати стійкість до загроз, але збільшення їх складності зменшує стійкість до антропогенних, техногенних і природних загроз.

2. Обізнаність (когнітивний процес)

2.1. Слід виокремити й адаптувати інформацію про КФС щодо позитивних та очікуваних дій людини для забезпечення відтворюваної реакції незалежно від походження або досвіду.

2.2. Отримати когнітивне розуміння (результат навчання) очікуваної оперативної поведінки на основі чіткого розуміння різниці між нормальними чи встановленими моделями поведінки та знанням того, що таких моделей немає.

2.3. Прихована й абстрактна інформація про КФС, доступна для певного кола осіб або доступна для потенційного порушника, інтегруючи активну реакцію і трансформацію КФС у відповідь на сприйняту загрозу.

Безпека та стійкість можуть бути найбільш критичними (важливими) характеристиками КФС, це спричинено наявністю кібер-компоненти [20]. Проектування системи безпеки КФС має ґрунтуватись на впровадженні комплексного і систематичного прогнозування чи виявлення кожної критичної для безпеки умови відмови через стан несправності або помилку людини, які можуть призвести до небезпеки та потенційної неузгодженості під час функціонування КФС. Ці процеси є відповіддю на вплив вимог щодо особливостей побудови системи безпеки або заходів для усунення й пом’якшення наслідків кібератаки. Сучасні процеси забезпечення безпеки системи ґрунтуються на оцінюванні ризику на основі вимог, функцій та критеріїв. Вони містять конкретні цілі, спрямовані на створення доказів, щоб перевірити, чи завжди функціонування системи безпеки призначено і забезпечує прийнятний ризик у фактичному робочому середовищі. Однак, системний аналіз безпеки повинен розвиватись проактивно, щоб враховувати загрози, спричинені кіберзахисними ситуаціями та сучасні методи кібератаки. Має бути розглянуто реалістичні моделі нападу з точки зору безпеки. Ними імітуються атаки, що є необхідним під час оцінювання їх впливу на фізичну і людську компоненту КФС.

Для багатьох механізмів контролю за кібербезпекою участь людини є доцільною. Оскільки КФС використовують автономні алгоритми прийняття рішень у реальному часі для контролю фізичного стану. Тому треба впроваджувати нові технології для проектування й аналізу систем безпеки, проте реагування та прийняття рішення може мати затримки в часі, які можуть загрожувати безпеці КФС. Цьому запобігти допомагають алгоритми виявлення та реагування в реальному часі, що є критично важливими для систем безпеки без урахування людського фактору, особливо зважаючи на важливі досягнення в теорії нелінійних і гібридних систем, для надійного, адаптивного, ігрово-теоретичного та відмовно-керувального контролю щодо проектування і розроблення алгоритмів для систем безпеки КФС.

КФС характеризуються їх взаємодією з робочим середовищем, як це зображено на рис. 3. Датчики разом або окремо вимірюють параметри середовища, потім виконують обчислення і дають вказівку на виконання певної дії, зазвичай змінюючи одну чи декілька властивостей робочого середовища, забезпечуючи таким чином контроль замкненого циклу (див. рис. 3). Архітектура повинна підтримувати різні режими взаємодії людини з КФС, щоб охоплювати різні ролі людини в функціонуванні КФС [21] - [23]:

– людина як контролер КФС або її партнер з управління;
– людина як користувач КФС;
– людина як споживач продукції КФС;
– людина як прямий об’єкт КФС, параметри стану якого слід вимірювати та діяти за необхідності.

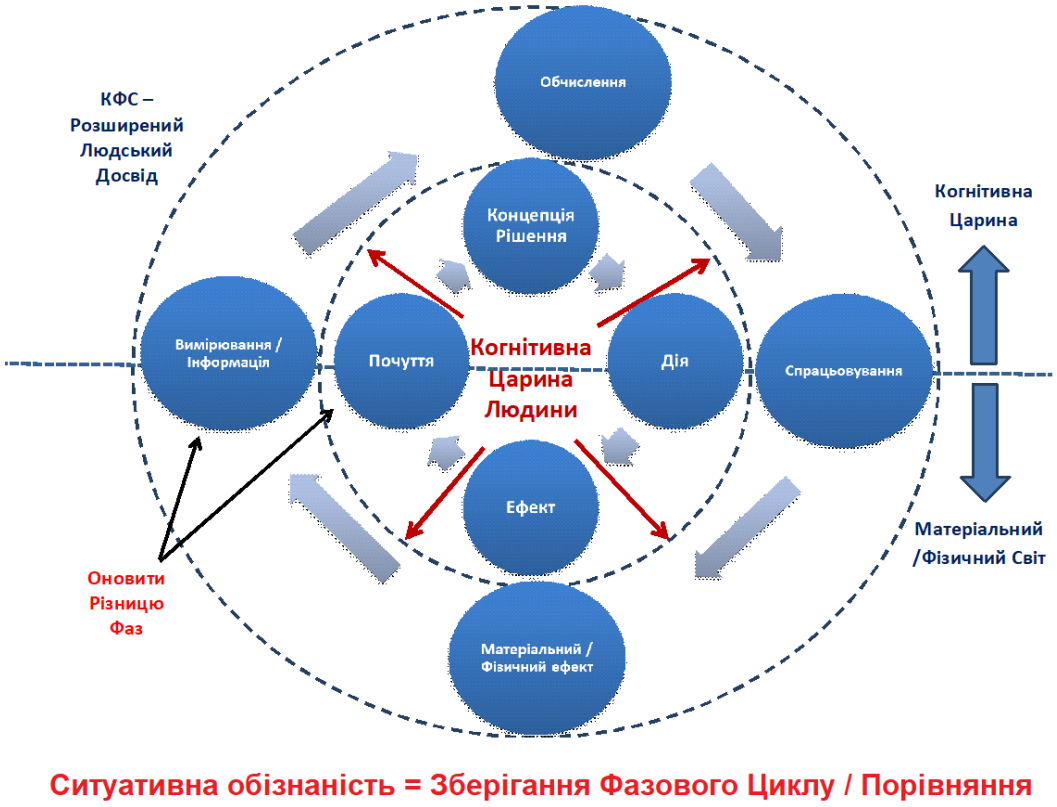

Рисунок 3 – Розширений когнітивний цикл КФС [13]

Здебільшого люди усвідомлюють обмеження своїх здібностей, тому КФС можна розглядати як технологію розширення і надання для них нових можливостей. Звичайно за таких умов, щоб забезпечити втілення КФС у сфери діяльності та повсякденний побут, потрібно мати оцінку невизначеності, що властива застосуванню КФС щодо наданих розширень. Людям потрібно мати певний рівень поінформованості про ситуацію та звичайно вони потребуватимуть захисту від помилок судження. Можливості людей розширюються за допомогою КФС, однак впевненість у функціонуванні КФС та оцінки рівня її надійності будуть важливими для успіху й прийняття допомоги КФС та збільшать їх користь для людства. У списку проблем, що стосуються КФС, найважливішими є теми, пов’язані зі взаємодією між оператором і КФС. Більш детальний розгляд (див. рис. 3) свідчить про те, що потрібно багато досліджень, щоб краще зрозуміти взаємозв’язок між когнітивним циклом діяльності людини та функціонуванням КФС, задуманим, побудованим та керованим людиною [13].

КФС інтегрують отриману фізичними компонентами інформацію для виконання заданих функцій, опрацювання якої залежить від часу та різного ступеня взаємодії з робочим середовищем, включаючи взаємодію з людьми.

Висновки. КФС – це концепція, орієнтована на домен (сферу застосування). КФС охоплюють визначені основоположні цілі, характеристики, загальні ролі та особливості їх застосування з урахуванням питань забезпечення кібербезпеки. Подальша робота з розвитку КФС пов'язана з уточненням архітектури високого рівня, що спрямована на усуненням проблем щодо їх впровадження, а також для визначення інтерфейсів для полегшення міжсекторальної сумісності КФС, щоб уможливити взаємодію між доменами (сферами застосування) та формувати системи систем. Використання КФС має бути ефективним і результативним, щоб задовольнити вимоги користувачів таких систем. Особливого занепокоєння з точки зору кібербезпеки зумовлюють характеристики КФС та як їх використовують люди: для пересічних користувачів – отримання нового рівня життя, для кіберзлочинців – шлях отримання прибутків. Поєднання фізичних і логічних компонентів в КФС буде створювати труднощі, щоб досягнути цілей зручності їх використання. Складність і різноманітність інтерфейсів може створювати значну проблему щодо навчання людської взаємодії з КФС.

Усунення людей від деталізації й дрібних етапів промислових процесів і підпроцесів – необхідність сьогодення, це незворотний процес еволюції. Кожна людина має впевнитись, що під час розроблення алгоритмів для систем безпеки, що їх створюють для таких платформ як кабінети здоров'я, кабінети споживачів під час оплати покупок і послуг тощо дотримано усіх превентивних заходів захисту. Ось тому є вельми пріоритетним завдання забезпечення кібербезпеки для КФС. Використання КФС не має викликати сумнівів у людей. Користувачі повинні бути впевненими, що дані їхнього приватного життя (картки пацієнтів закладів охорони здоров'я, список транзакцій банківських карток, особисте листування і хобі вільного часу, зокрема перегляд сторінок Інтернету, улюблені закладки браузера, що ілюструють, наприклад зацікавленість, ідентичність і громадянську позицію) захищено.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Промисловість 4.0 – Підхід Компанії Advantech. [Електронний ресурс]. Доступно: https://www.proxis.ua/uk/show-article/100/. Дата звернення: Жовт. 06, 2019.

[2] H. Kagermann, W.-D. Lukas, and W. Wahlster, "Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution", *VDI nachrichten*, № 13, 2011. [Online]. Available: http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-DingeWeg-4-industriellen-Revolution. Accessed on: Жовт. 06, 2019.

[3] I. Horváth, and Bart H. M. Gerritsen, "Cyber-physical systems: concepts, technologies and implementation principles", in *Proc. 9th International Symposium on Tools and Methods of Competitive Engineering (TMCE)*, Karlsruhe, Germany, May 7-11, pp. 19-36, 2012.

[4] В. Дудикевич, Г. Микитин, та А. Ребець, "Квінтесенція інформаційної безпеки кіберфізичної системи", *Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі*, № 887, с. 58-68, 2018.

[5] G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems", *Control Theory and Technology*, vol. 14, no. 1, pp. 2-10, 2016, doi: 10.1007/s11768-016-5123-9.

[6] А. Мельник, "Кіберфізичні системи: проблеми створення та напрями розвитку", *Вісник Національного університету "Львівська політехніка": Комп'ютерні системи та мережі,* № 806, с. 154-161, 2014.

[7] В. Чунжі, С. Яцишин, О. Лиса, та А-В. Мідик, "Кіберфізичні системи та їх програмне забезпечення", *Вимірювальна техніка та метрологія*, № 79 (1), с. 34-38, 2018.

[8] В. Дудикевич, Г. Микитин, та А. Ребець, "Комплексна система безпеки кіберфізичної системи "iPhone – Wi-Fi, Bluetooth – давачі", *Системи обробки інформації*, № 2 (148), с. 84-87, 2017, doi: 10.30748/soi.2017.148.16.

[9] О. Єршова, В. Одноволик, та Л. Бажан, "Кіберфізичні системи як основа смарт-економіки", *Науковий вісник Національної академії статистики, обліку та аудиту*, № 1-2, с. 69-79, 2019.
[10] В. Вітлінський, та В. Скіцько, "Ризики в Індустрії 4.0", *Вісник Черкаського університету*, № 3, с. 17-26, 2016.
[11] N. Makitalo et al., "Social Devices: Collaborative Co-located Interactions in a Mobile Cloud", in *Proc. 11th International Conference Mobile and Ubiquitous Multimedia*, pp. 1-10, 2012, doi: 10.1145/2406367.2406380.
[12] Н. Казакова, Ю. Щербина, та О. Фразе-Фразенко, "Проблеми безпеки сучасних кіберфізичних систем", на *міжнародній науково-практичній конференції Кібербезпека в Україні: правові та організаційні питання*, Одеса, Україна, Листоп. 22, 2019, с. 77-78.
[13] Framework for Cyber-Physical Systems: vol. 1, Overview, doi: 10.6028/NIST.SP.1500-201.
[14] F. B. Schneider, ed., "Trust in cyberspace". *National Research Council*. [Online]. Available: http://www.nap.edu/catalog/6161/trust-in-cyberspace. Accessed on: Oct. 06, 2019.
[15] A. Colombo, and T. Bangemann, "Industrial Cloud-based Cyber-physical Systems: The IMC-AESOP Approach". *Cham Springer International Publishing*, 2014.
[16] D. Kahneman, and A. Tversky, "On the reality of cognitive illusions", *Psychological Review* 103 (3). pp. 582-591, 1996.
[17] M. Hilbert, "Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making", *Psychological Bulletin*, no. 138 (2), pp. 211-237, 2012, doi: 10.1037/a0025940.
[18] M. Haselton, D. Nettle, and P. Andrews, "The evolution of cognitive bias", in D. M. Buss, ed. *The Handbook Of Evolutionary Psychology: Hoboken*, NJ, US: John Wiley & Sons Inc. pp. 724-746, 2005, doi: 10.1002/9780470939376.ch25.
[19] О. Булигіна, "Дослідження користувачів та супутні когнітивні ілюзії". [Електронний ресурс]. Доступно: https://telegraf.design/doslidzhennya-korystuvachiv-ta-suputni-kognityvni-ilyuziyi/. Дата звернення: Жовт. 06, 2019.
[20] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *Dependable and Secure Computing, IEEE Transactions*. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1335465&url= http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1335465. Accessed on: Oct. 06, 2019.
[21] Framework for Cyber-Physical Systems: vol. 2, Working Group Reports, doi: 10.6028/NIST. SP.1500-202.
[22] Cyber-Physical Systems. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems. Accessed on: Oct. 06, 2019.
[23] S. Zanero, and P. di Milano, "Cyber-Physical Systems", *Computer*, vol. 50, pp. 14-16, doi: 10.1109/MC.2017.105.

Стаття надійшла до редакції 29.01.2020.

REFERENCE

[1] Industry 4.0 – Company Approach "Advantech". [Online]. Available: https://www.proxis.ua/uk/show-article/100/. Date of application: Oct. 06, 2019.
[2] H. Kagermann, W.-D. Lukas, and W. Wahlster, "Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution", *VDI nachrichten*, № 13, 2011. [Online]. Available: http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-DingeWeg-4-industriellen-Revolution. Accessed on: Oct. 06, 2019.
[3] I. Horváth, and Bart H. M. Gerritsen, "Cyber-physical systems: concepts, technologies and implementation principles", in *9th International Symposium on Tools and Methods of Competitive Engineering (TMCE)*, Karlsruhe, Germany, May 7-11, pp. 19-36, 2012.

[4] V. Dudykevych, G. Mykytyn, and A. Rebets, "The quintessence of information security of the cyberphysical system", *Bulletin of Lviv Polytechnic National University series: "Information Systems and Networks"*, no. 887, pp. 58-68, 2018.

[5] G. Wu, J. Sun, and J. Chen, "A survey on the security of cyber-physical systems", *Control Theory and Technology*, vol. 14, no. 1, pp. 2-10, 2016, doi: 10.1007/s11768-016-5123-9.

[6] A. Melnyk, "Cyberphysical systems: problems of creation and directions of development", *Bulletin of Lviv Polytechnic National University series: "Computer Systems and Network"*, no. 806, pp. 154-161, 2014.

[7] W. Chunzhi, S. Yatsyshyn, O. Lysa, and A-V. Midik, "Cyberphysical systems and their software", *Measuring Equipment and Metrology*, no. 79 (1), pp. 34-38, 2018.

[8] V. Dudykevych, G. Mykytyn, and A. Rebets, "Integrated security system of the cyberphysical system "iPhone-Wi-Fi, Bluetooth-sensors", *Information Processing Systems*, no. 2 (148), pp. 84-87, 2017, doi: 10.30748/soi.2017.148.16.

[9] O. Yershova, V. Odnovolyk, and L. Bazhan, "Cyberphysical systems as the basis of smart economy", *Scientific Bulletin of the National Academy of Statistics, Accounting and Audit*, no. 1-2, pp. 69-79, 2019.

[10] V. Vitlinsky, and V. Skitsko, "Risks in Industry 4.0", *Cherkasy University Bulletin*, no. 3, pp. 17-26, 2016.

[11] N. Makitalo et al., "Social Devices: Collaborative Co-located Interactions in a Mobile Cloud", in *Proc. 11th International Conference Mobile and Ubiquitous Multimedia*, pp. 1-10, 2012, doi: 10.1145/2406367.2406380.

[12] N. Kazakova, Y. Shcherbyna, and O. Fraze-Frazenko, "Problems of security of modern cyberphysical systems", on *International Science Practice Conference Cybersecurity in Ukraine: legal and organizational issues*, Odessa, Ukraine, Nov. 22, 2019, pp. 77-78.

[13] Framework for Cyber-Physical Systems: vol. 1, Overview, doi: 10.6028/NIST.SP.1500-201.

[14] F. B. Schneider, ed., "Trust in cyberspace". *National Research Council*. [Online]. Available: http://www.nap.edu/catalog/6161/trust-in-cyberspace. Accessed on: Oct. 06, 2019.

[15] A. Colombo, and T. Bangemann, "Industrial Cloud-based Cyber-physical Systems: The IMC-AESOP Approach". *Cham Springer International Publishing*, 2014.

[16] D. Kahneman, and A. Tversky, "On the reality of cognitive illusions", *Psychological Review* 103 (3). pp. 582-591, 1996.

[17] M. Hilbert, "Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making". *Psychological Bulletin*, no. 138 (2), pp. 211-237, 2012 doi: 10.1037/a0025940.

[18] M. Haselton, D. Nettle, and P. Andrews, "The evolution of cognitive bias", in D. M. Buss, ed. *The Handbook Of Evolutionary Psychology: Hoboken*, NJ, US: John Wiley & Sons Inc. pp. 724-746, 2005, doi: 10.1002/9780470939376.ch25.

[19] O. Bulygina, "User research and associated cognitive illusions". [Online]. Available: https://telegraf.design/doslidzhennya-korystuvachiv-ta-suputni-kognityvni-ilyuziyi/. Accessed on: Oct. 06, 2019.

[20] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *Dependable and Secure Computing, IEEE Transactions*. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1335465&url= http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1335465. Accessed on: Oct. 06, 2019.

[21] Framework for Cyber-Physical Systems: vol. 2, Working Group Reports, doi: 10.6028/NIST.SP.1500-202.

[22] Cyber-Physical Systems. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems. Accessed on: Oct. 06, 2019.

[23] S. Zanero, and P. di Milano, "Cyber-Physical Systems", *Computer*, vol. 50, pp. 14-16, doi: 10.1109/MC.2017.105.

YULIIA KOZHEDUB,
YULIIA KRAMSKA,
VIRA HYRDA

ANALYSIS OF THE HUMAN FACTOR INFLUENCE ON THE CYBER-PHYSICAL SYSTEM

The issue of rapid application of the Fourth Industrial Revolution technologies for different aspects of human life, which summarizes various technical means and information technologies through the implementation of cyber-physical systems, cyber-physical production systems, and the Internet of Things in the production of goods and services. The widespread use of cyber-physical systems as a new mechanism and a way to achieve a new, higher standard of living is analyzed. Cyber-physical systems collect, store, and analyze data from sensors. This is necessary to provide generalized information and then use it to combine virtual and physical environments. The purpose of such integration is to create a network environment in which intelligent objects interact with each other. Currently, cyber-physical systems ensure the integration of computing facilities into physical processes, and in the future, such systems will provide for the introduction of artificial intelligence elements into control processes. This is necessary because man is no longer able to provide effective management within the existing automated systems of extremely complex production, technological, and social processes. Emphasis is placed on the risks of cyber-physical systems and the importance of dealing with them is shown. Their classification taking into account the influence of the application of the technologies of the Fourth Industrial Revolution with the use of cyber-physical systems is given. This classification covers the components that reflect each component of the innovation concept – the Fourth Industrial Revolution. The main causes of errors in the functioning of "man-machine" systems to human bias have been studied. Cyber-physical systems have been found to include interdependent analog, digital, physical, and human components designed to function with integrated physical devices and logic elements. The definition of the term "cognitive bias" is given. It is stated that cyber-physical systems have nine aspects, which are called "problem clusters". The advantages and disadvantages of using the latest technologies of the Fourth Industrial Revolution will depend on the need to assess the balance of "benefit-security" for the evolutionary process in general and the individual in particular.

Keywords: Fourth Industrial Revolution, cyber-physical system, human-machine system, human factor, bias, risks, cybersecurity.

Кожедуб Юлія Василівна, кандидат технічних наук, старший науковий співробітник, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-6181-5519.

E-mail: JuliaKozhedub@email.ua.

Крамська Юлія Альфредівна, старший інженер, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-6279-0464.

E-mail: kramska_ua@ukr.net.

Гирда Віра Анатоліївна, старший інженер, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-3858-4086.

E-mail: gidraponka@ukr.net.

Kozhedub Yuliia, candidate of technical sciences, senior research, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Kramska Yuliia, senior engineer, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Hyrda Vira, senior engineer, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.